Informationelle Selbstbestimmung in sozialen Netzwerken:

Mehrseitige Rechtsbeziehungen und arbeitsteilige Verantwortungsstrukturen als Herausforderung für das europäisierte Datenschutzrecht

Dissertation

zur Erlangung des Grades eines Doktors des Rechts

bei der Bucerius Law School in Hamburg

vorgelegt von:

Barbara Elisabeth Schunicht

Hamburg, Januar 2018

Tag der Promotion: 17. Januar 2018

Erstreferent: Herr Prof. Dr. Michael Fehling

Zweitreferentin: Frau Prof. Dr. Marion Albers

Meiner Familie

Vorwort

Die vorliegende Arbeit wurde unter der Betreuung von Herrn Prof. Dr. Michael Fehling an der Bucerius Law School in Hamburg angefertigt und im Juli 2017 von der Bucerius Law School als Dissertation angenommen. Rechtsprechung und Literatur wurden umfassend bis Oktober 2016 berücksichtigt. Nachfolgende gesetzliche Änderungen, insbesondere der Erlass des DSAnpUG-EU im Juni 2017, wurden in Hinweisen eingearbeitet.

Mein besonderer Dank gilt meinem Doktorvater Herrn Prof. Dr. Michael Fehling, welcher mich bei der Anfertigung der Arbeit stets unterstützt hat und mir mit tatkräftigem Rat zur Seite stand. Ihm wie auch meinen Kollegen danke ich sehr für die langen und interessanten Diskussionen, die zu wertvollen Anregungen und Einsichten für diese Arbeit geführt haben. Darüber hinaus möchte ich Herrn Prof. Dr. Michael Fehling und Frau Prof. Dr. Marion Albers von der Universität Hamburg sehr für die schnelle Erstellung der beiden Gutachten danken.

Keine Danksagung wäre zudem vollständig ohne meiner Familie und meinen Freunden von Herzen zu danken. Sie waren zu jeder Zeit für mich da und hatten immer ein offenes Ohr für meine Sorgen und Zweifel. Ohne ihre unbedingte Unterstützung wäre es mir nicht möglich gewesen, diese Arbeit zu schreiben und fertig zu stellen.

In einer bewussten Entscheidung wurde diese Arbeit als eDissertation mit Open Access im Internet veröffentlicht. In einer zunehmend digitalisierten und vernetzten Welt erscheint dies als ein zeitgemäßer Weg, eine rechtswissenschaftliche Dissertation allgemein zugänglich zu machen, die sich mit aktuell politisch relevanten Fragestellungen des Internets auseinandersetzt und damit auch Themenbereiche berührt, die letztlich Forschungsgegenstand anderer Wissenschaften, insbesondere der Informatik, sein müssen. Eine allgemeine Zugänglichkeit kann dem interdisziplinären Ideenaustausch dabei nur förderlich sein und erscheint mir daher in diesem Kontext als die angemessene Form der Veröffentlichung.

Hamburg, 9. Januar 2018 *Barbara E. Schunicht*

Inhaltsübersicht

Inhaltsverzeichnis

Seite

Seite

Seite

Seite

A. Einleitung

Im Zeitalter ubiquitärer Datenverarbeitung wandelt sich das Datenschutzrecht von einer rechtlichen Nische zu einer für die individuelle Freiheitssicherung unabdingbaren und grundlegenden Querschnittsmaterie. Bereits 1983 stellte das Bundesverfassungsgericht fest, dass „Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[1] Schon damals sah das Gericht diese Selbstbestimmung durch die aufkommende automatische Datenverarbeitung als gefährdet an, indem aus einer fehlenden individuelle Kontrolle über die eigenen Daten reale Freiheitseinschränkungen durch Abschreckungseffekte resultieren könnten. Das Gericht erkannte eine Gefährdung des allgemeinen Persönlichkeitsrechts gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in einer bis dahin nicht bekannten Ausprägung und konstatierte: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“[2]

Die Möglichkeiten und Methoden der Datenverarbeitung, die vor über 30 Jahren Anlass zu diesen Worten gaben, wirken aus heutiger Sicht nachgerade steinzeitlich. An die Stelle von staatlichen Großrechneranlagen sind Geodaten, elektronische Bezahlsysteme, RFID-Chips und insbesondere das Internet mit all seinen Kommunikations- und Interaktionsmöglichkeiten, sowie Metadaten getreten. Die rasante Verbesserung von Speicher- und Rechenkapazitäten ermöglicht im Rahmen von Big Data Analysen die Auswertung ungeahnter Datenmengen und das Herausarbeiten von statistischen Mustern, die auf ahnungslose Individuen übertragen werden können.[3] Das freiheitseinschränkende Potential der allgegenwärtigen Datenverarbeitung ist somit größer denn je und damit auch die Herausforderung an das Datenschutzrecht und andere Rechtsgebiete, dennoch die grundlegende Freiheit der informationellen Selbstbestimmung zu gewährleisten.[4]

Ein besonders aktuelles und relevantes Gebiet der selbstbestimmungsgefährdenden Datenverarbeitung sind soziale Netzwerke im Internet. Während diese unzweifelhaft gewisse

---

1 BVerfGE 65, 1 (43) – Volkszählung.
2 BVerfGE 65, 1 (43) – Volkszählung.
3 Ausführlich: *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 13 ff.
4 Instruktiv: *Martini*, DVBl. 2014, 1481 (1482 ff.); *Sandfuchs*, Privatheit wider Willen, S. 30 ff., 46 ff.; *Mayer-Schönberger*, Die Tugend des Vergessens, S. 130 ff.

Vorteile für ihre Nutzer bieten, weisen sie auch das Potential für die Erstellung umfassender Persönlichkeitsprofile auf, deren Einsatzmöglichkeiten weit über personifizierte Werbung hinausgehen. Sie geben zudem Individuen die Möglichkeit, mit geringem Aufwand und zugleich einer sehr hohen Reichweite Daten und Informationen über Dritte zu verbreiten und diese damit möglicherweise zu schädigen, jedenfalls aber in ihrer informationellen Selbstbestimmung zu beeinträchtigen. Dies gilt insbesondere für die nicht autorisierte Verbreitung von privaten oder intimen Informationen, aber auch von falschen Behauptungen oder Unterstellungen.

Gegenstand der Arbeit ist die Frage, inwieweit das allgemeine Datenschutzrecht den Herausforderungen begegnen kann, die soziale Netzwerke für die informationelle Selbstbestimmung des Einzelnen darstellen. Ausgangspunkt der Untersuchung sind hierbei die einschlägigen Bestimmungen der europäischen Datenschutzgrundverordnung (DS-GVO)[5], welche ab dem 25.5.2018 das bisherige nationale Recht ersetzen werden. Soweit dies für die zukünftige Rechtslage noch von Bedeutung ist – beispielsweise für eine dogmatische Einordnung unbestimmter Rechtsbegriffe in der DS-GVO – wird zudem vertieft auf die bisher geltenden nationalen Regelungen des Bundesdatenschutzgesetzes (BDSG), des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) eingegangen, welche auf die europäische Datenschutzrichtlinie (DSRL)[6] aus dem Jahre 1995 zurückgehen. An geeigneter Stelle wird zudem auf die Regelungen des BDSG n.F. gemäß Art. 1 DSAnpUG-EU eingegangen.

Die Untersuchung beginnt mit einem kurzen Überblick über die gesellschaftliche Verbreitung sozialer Netzwerke und die mit ihnen verbundenen Datensammlungen und hieraus resultierende Konsequenzen und Risiken (B.). Hierbei wird schwerpunktmäßig auf die Datenverarbeitung durch private Akteure geschaut, während staatliche Datenverarbeitung der weiteren Forschung überlassen bleiben soll.

Anschließend werden kollisionsrechtliche Fragestellungen beantwortet, die insbesondere in Bezug auf Facebook bestehen (C.). Diese Fragen sind aktuell von erheblicher praktischer

---

5 Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Nachfolgende Zitationen der DS-GVO beziehen sich auf diese Endfassung, soweit nicht ausdrücklich auf einen der vorigen Entwürfe Bezug genommen wird.

6 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.

Bedeutung und auch Gegenstand eines vom Bundesverwaltungsgericht angestrengten Vorabentscheidungsverfahrens vor dem EuGH.[7] Zwar wird durch die Geltung der DS-GVO ab dem 25.5.2018 eine Vereinheitlichung des materiellen Datenschutzrechts eintreten; wie gezeigt werden wird, bleibt eine Beantwortung dieser Fragen aber auch zukünftig sehr relevant, um die Zuständigkeit der nationalen Aufsichtsbehörden zu bestimmen. Ferner sind wichtige Elemente des datenschutzrechtlichen Verantwortlichkeitsbegriffs, welcher im Zentrum der Arbeit steht, im Zusammenhang mit dem kollisionsrechtlichen Begriff der „verantwortlichen Stelle" entwickelt und geprägt worden. Auch deshalb ist es geboten, selbst nach Verabschiedung der DS-GVO die hiermit verbundenen bisherigen kollisionsrechtlichen Fragen detailliert zu untersuchen und zu beantworten.

Der Schwerpunkt der Arbeit liegt anschließend auf der Analyse der Akteursgeflechte in sozialen Netzwerken im Hinblick auf eine mögliche datenschutzrechtliche Verantwortlichkeit (D.I.). Ausgehend von den unterschiedlichen Beteiligten wird untersucht, wie das klassisch dichotome Datenschutzrecht mit Problemen wie arbeitsteiliger Datenverarbeitung oder datenverarbeitenden Nutzern umgehen kann. Die Möglichkeit der Zuweisung datenschutzrechtlicher Verantwortlichkeit an die einzelnen Akteure als Anknüpfungspunkt für mögliche Rechte und Pflichten erweist sich hierbei als Grundvoraussetzung jeglicher späteren Überlegung einer effektiven Regulierung der stattfindenden Datenverarbeitung.

Als problematisch erweist sich weiterhin das in § 13 Abs. 6 TMG garantierte Recht auf anonyme oder jedenfalls pseudonyme Nutzung von Diensteangeboten (D.II.). Sowohl mit Blick auf mögliche Impressumspflichten gemäß § 5 Abs. 1 TMG als auch die Zumutbarkeit einer anonymen Registrierung für den Anbieter des sozialen Netzwerks erweisen sich die erhöhten Datenverarbeitungsmöglichkeiten durch Nutzer als rechtliche Herausforderung. Da ein Recht auf anonyme oder pseudonyme Nutzung nicht ausdrücklich in der DS-GVO normiert ist, aber dennoch in manchen Regelungen angesprochen wird, gilt es zudem zu untersuchen, inwieweit dieses Recht zukünftig noch Bestand haben wird.

Zum Abschluss soll das in sozialen Netzwerken regelmäßig existierende Informations- und Machtgefälle in den Blick genommen werden (D.III.). Exemplarisch wird die Leistungsfähigkeit der Einwilligung als freiheitssicherndem Instrument untersucht, welche sowohl nach geltendem Recht als auch nach der DS-GVO eine zentrale Rolle einnimmt. Als

[7] BVerwG, ZD 2016, 393 (393 ff.).

flankierende Maßnahmen werden insbesondere Möglichkeiten des Selbstdatenschutzes und des sogenannten „Risk-Based“ Approach als Regulierungsstrategien betrachtet.

Im Umfang eines Ausblicks wird zuletzt von den bis dahin erlangten Erkenntnissen abstrahiert und eine abstrakte Bewertung des Datenschutzrechts im Angesicht der Herausforderungen der modernen Datenverarbeitung, insbesondere in sozialen Netzwerken gewagt. Die Steuerungsfähigkeit des Datenschutzrechts wird an den Herausforderungen der Internationalität und Multipolarität der Datenverarbeitung gemessen und die Möglichkeit und Angemessenheit einer technologieneutralen Regulierung – wie dies nicht zuletzt das Ziel der DS-GVO ist – hinterfragt (E.I.). In Anknüpfung an die hierzu in den letzten Jahren erschienene umfangreiche Literatur werden zudem das Spannungsfeld der Einwilligung zwischen befreiender Selbstbestimmung und überfordernder Selbstentmündigung näher betrachtet und Konsequenzen für die Regulierung sozialer Netzwerke gezogen.

Am Ende steht ein Fazit (0.), das die Angemessenheit des bisherigen und zukünftigen europäisierten Datenschutzrechts zur Sicherung der informationellen Selbstbestimmung in den untersuchten Fragestellungen in sozialen Netzwerks zusammenfassend beurteilt.

B. Profilbildungs- und Überwachungspotentiale in sozialen Netzwerken

I. Gesamtgesellschaftliche Verbreitung sozialer Netzwerke

1. Untersuchungsgegenstand: Begriff des sozialen Netzwerks

Der Begriff der „sozialen Netzwerke" hat sich mittlerweile allgemeinsprachlich etabliert für Internetanwendungen wie Facebook, Google +, Xing, LinkedIn oder MeinVZ.[8] Eine genaue wissenschaftliche Definition und Abgrenzung gestaltet sich allerdings schwierig. Prägende Elemente sind zweifellos die Möglichkeit zur individuellen Selbstdarstellung durch ein Profil und eine Infrastruktur zur Kommunikation und Interaktion der Nutzer untereinander.[9] Diese funktionelle Betrachtung ermöglicht aber nur eine sehr unscharfe Abgrenzung zu anderen Web 2.0 Anwendungen wie etwa Weblogs oder Diskussionsforen, die ebenfalls Profile ihrer Nutzer beinhalten und Kommentarfunktionen bieten.[10] Für die Zwecke dieser Arbeit soll von einem eher weiten Verständnis digitaler sozialer Netzwerke ausgegangen werden, welche dem allgemeinsprachlichen Gebrauch des Begriffs entspricht. Ein soziales Netzwerk stellt dementsprechend eine Internetanwendung dar, bei der Nutzer sich zunächst registrieren und dann ein zumindest semi-öffentliches Profil erstellen müssen, das gegebenenfalls nur für Kontakte innerhalb des sozialen Netzwerks sichtbar ist, mit dem sie anschließend mit anderen Nutzern interagieren und kommunizieren können. Die eigene Selbstdarstellung und soziale Interaktion mit anderen Nutzern soll grundsätzlich im Vordergrund des allgemeinen Nutzungszwecks stehen, anders als beispielsweise bei reinen Multimediaplattformen wie YouTube, bei welchen eine Interaktion mit anderen Personen zwar auch möglich ist, aber hinter dem Teilen von Inhalten deutlich zurücktritt.[11] Graubereiche nach dieser Definition sind Dienste wie Twitter oder Instagramm, die nicht ganz so stark wie etwa Facebook auf eine umfassende digitale Selbstdarstellung ausgerichtet sind, sondern mehr auf eine partielle Selbstdarstellung durch das Veröffentlichen von kurzen Gedanken oder Fotos. Auch hier steht indes die Interaktion und die Selbstdarstellung gegenüber anderen registrierten Nutzern und

---

8 Vgl. *Neuberger*, in: Neuberger/Gehrau (Hrsg.), Soziale Netzwerke, S. 37; Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 3 ff.; *Piltz*, Soziale Netzwerke, S. 19.

9 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 20; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 311 f.; *Neumann-Braun/Autenrieth*, in: Freundschaft und Gemeinschaft im Social Web (Ders./Dies. (Hrsg.)), S. 10; *Piltz*, Soziale Netzwerke, S. 19 f.; *Maisch*, Informationelle Selbstbestimmung, S. 161 f.

10 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 20; vgl. auch *Neuberger*, in: Neuberger/Gehrau (Hrsg.), Soziale Netzwerke, S. 34 ff.

11 Vgl. auch *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 20 f.; *Chmelik*, Social Network Sites, S. 202 ff.; *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner, S. 424.

Kontakten im Vordergrund, während sich über die Zeit hinweg durch das Nutzerverhalten Persönlichkeitsprofile für den Anbieter anlegen lassen. Die Risikolage ist mithin zumindest sehr vergleichbar mit „klassischen" sozialen Netzwerken wie Facebook oder früher schon MySpace, so dass sie in dieser Arbeit ebenfalls vom Begriff der sozialen Netzwerke mitumfasst sein sollen.[12]

Der hier verwendete Begriff der sozialen Netzwerke soll nicht verwechselt werden mit dem weiteren sozialwissenschaftlichen Begriffsverständnis, in welchem er überall, also auch außerhalb des Internets existierende soziale Geflechte von Akteuren bezeichnet.[13] Zur Vermeidung begrifflicher Unklarheiten wird daher von einigen Autoren vorgeschlagen, von „sozialen Netzwerkplattformen" zu sprechen[14] oder von sozialen Netzwerkdiensten, sozialen Netzwerkseiten oder Online-Communities.[15] Angesichts der mittlerweile weit verbreiteten Bezeichnung als soziale Netzwerke soll indes dieser Begriff im oben beschriebenen Verständnis im Folgenden verwendet werden.

Soweit auf technische Details rekurriert wird, wird schwerpunktmäßig Facebook als das weltweit und auch in Deutschland am weitesten verbreitete soziale Netzwerk als Beispiel herangezogen. Da die Funktionalitäten häufig vergleichbar sind, ist im Allgemeinen aber davon auszugehen, dass die rechtliche Bewertung anderer Dienste ähnlich ausfallen würde.[16]

2. Überblick: Entwicklung und Verbreitung sozialer Netzwerke

Die Ursprünge moderner, digitaler sozialer Netzwerke liegen länger zurück, als man spontan denken könnte, nämlich Ende der 80er, Anfang der 90er Jahre. Die Anwendungen AOL, Prodigy und CompuServe ermöglichten – noch innerhalb von geschlossenen Netzwerken, nicht dem Internet, wie es heute bekannt ist –, eigene Profile zu erstellen, Veranstaltungen zu veröffentlichen und private Nachrichten zu verschicken.[17] 1995 wurde in den USA das Netzwerk Classmates.com gegründet, um eine Pflege alter Schulfreund- und Bekanntschaften zu ermöglichen. Heute hat das Netzwerk nach eigenen Angaben über 50 Mio. Mitglieder.[18]

---

12 Anders für Twitter und andere Microblogging-Dienste: *Chmelik*, Social Network Sites, S. 210 f., da es unmöglich sei, einen eigenen Freundeskreis zu definieren und stattdessen die Informationsverbreitung und -gewinnung in der Öffentlichkeit zu stark im Vordergrund stünde.

13 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 19.

14 So *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 19 ff.

15 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 19; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 311.

16 Vgl. *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 67.

17 Ausführlich https://de.wikipedia.org/wiki/Soziales_Netzwerk_(Internet).

18 http://www.classmates.com/.

Wirklich an Reichweite und Bedeutung gewannen soziale Netzwerke aber erst Anfang bis Mitte der 2000er Jahre, insbesondere durch die zunehmende weltweite Nutzung des Internets.[19] 2002 wurde das Netzwerk LinkedIn gegründet, im Juli 2003 folgten MySpace und Anfang 2004 Xing sowie das heute weltweit größte Netzwerk Facebook. 2011 gründete Google sein Netzwerk Google +.[20] Zudem gab und gibt es zahlreiche eher regional bzw. national begrenzte soziale Netzwerke. Im Jahr 2005 wurde beispielsweise das ehemals sehr erfolgreiche deutsche Netzwerk StudiVZ gegründet, 2007 ergänzt um SchülerVZ und 2008 um MeinVZ für nicht-akademische Nutzer.[21] In China ist das soziale Netzwerk Qzone seit 2005 online und mit 640 Millionen Nutzern (Stand Dezember 2015)[22] eins der größten internationalen sozialen Netzwerke. Hierbei ist anzumerken, dass zahlreiche internationale Netzwerkplattformen in China durch die staatliche Zensurpolitik gesperrt und somit nicht ohne weiteres für Nutzer erreichbar sind[23], was den nationalen Anbietern einen erheblichen Wettbewerbsvorteil verschafft. Weitere Beispiele für soziale Netzwerke sind das vor allem in Großbritannien verbreitete Netzwerk Bebo, Orkut in Brasilien, Vkontakte in Russland und Mixi in Japan.[24]

Das derzeit weltgrößte Netzwerk Facebook verzeichnete im August 2008 100 Millionen aktive Mitglieder[25], im Juli 2010 waren es bereits eine halbe Milliarde. Die Marke von einer Milliarde Nutzern wurde im Oktober 2012 überschritten.[26] Im ersten Quartal von 2016 waren 1,65 Milliarden Nutzer bei Facebook aktiv.[27] Damit wäre rein rechnerisch mehr als 20% der gesamten Weltbevölkerung Mitglied bei Facebook; wobei freilich von der Existenz von zahlreichen Doppelaccounts auszugehen ist.

Auch wenn soziale Netzwerke in Grundzügen schon relativ früh existierten, lässt sich daher festhalten, dass sie erst ab Mitte der 2000er einer breiten Bevölkerungsschicht bekannt und intensiver genutzt wurden. Sie stellen damit ein verhältnismäßig junges Phänomen des Internets dar.

---

19 So auch *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 21.

20 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 23; *Neumann-Braun/Autenrieth*, in: Freundschaft und Gemeinschaft im Social Web (Ders./Dies. (Hrsg.)), S. 10.

21 *Niemann/Schenk*, in: Digitale Privatsphäre, S. 23; *Neumann-Braun/Autenrieth*, in: Ders./Dies. (Hrsg.), Freundschaft und Gemeinschaft im Social Web, S. 10 f.

22 Tecent, Annual Report 2015, S. 6.

23 *Niemann/Schenk*, in: Digitale Privatsphäre, S. 24.

24 *Niemann/Schenk*, in: Digitale Privatsphäre, S. 24.

25 http://www.heise.de/newsticker/meldung/Facebook-meldet-100-Millionen-Nutzer-200097.html; vgl. auch http://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/.

26 http://www.heise.de/newsticker/meldung/Facebook-hat-eine-Milliarde-aktive-Nutzer-1723387.html; vgl. auch http://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/.

27 http://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/.

Der Schwerpunkt der Beispiele in dieser Arbeit wird sich – wie oben bereits angedeutet – auf Facebook beziehen, welches auch in Deutschland nach repräsentativen Untersuchungen des Branchenverbandes Bitkom aus dem Jahr 2013 das mit Abstand am meisten genutzte soziale Netzwerk ist: 56% der deutschen Internetnutzer verwenden hiernach Facebook, womit ein Zuwachs von 11% gegenüber dem Jahre 2011 festzustellen ist.[28] In der Gruppe der 14 bis 19-Jährigen sind hiernach 83% bei Facebook registriert und aktiv, Google+ als dichtester „Verfolger" liegt abgeschlagen bei 29%, Twitter bei 22%. Unter den 30 bis 49-Jährigen kommt Facebook immerhin auf einen Anteil von 58% registrierten und 51% aktiven Nutzern, bei den 50-Jährigen und älteren auf 53% registrierte, bzw. 40% aktive Nutzer. Auch in diesen Gruppen sind die „Verfolger" Stayfriends und Wer-kennt-wen mit ca. 26%, bzw. 19% registrierten und jeweils nur ca. 11% aktiven Nutzern weit abgeschlagen. Google+ kommt in diesen Gruppen auf gerade einmal einen Anteil von 14% registrierten und weniger als 6% aktiven Nutzern.[29] Insgesamt sollen 78% der deutschen Internetnutzer in mindestens einem sozialen Netzwerk registriert und 67% hiervon aktive Nutzer sein[30], was die Verbreitung und Bedeutung sozialer Netzwerke in der Gesellschaft unterstreicht. Größere Differenzen bestehen erwartungsgemäß zwischen den Generationen: Während von den 14 bis 29-Jährigen 93% in mindestens einem sozialen Netzwerk registriert sind und dieses auch aktiv nutzen, gibt es bei den 65-Jährigen und älteren nur 66% registrierte und 47% aktive Nutzer.[31] Auch diese Zahl mag allerdings in ihrer Höhe durchaus zu überraschen.

II. Datenauswertung und Profilbildung in sozialen Netzwerken

Die Nutzung sozialer Netzwerke erzeugt eine erhebliche Menge an unterschiedlichen Daten. Viele von diesen Daten erlauben detaillierte Rückschlüsse auf die Persönlichkeit, das Verhalten, die Lebensumstände und die Interessen der Nutzer. Indem sie diese Rückschlüsse zulassen, sind sie Informationsgrundlagen, aus denen Informationen gewonnen werden können.

---

28 https://www.bitkom.org/Publikationen/2013/Studien/Soziale-Netzwerke-dritte-erweiterte-Studie/SozialeNetzwerke-2013.pdf, S. 11. Zu etwas niedrigeren Zahlen bei einer größeren Teilnehmerbasis kommt Statista für den Zeitraum von Oktober 2013 bis April 2014, wonach lediglich 41% der deutschen Bevölkerung Facebook nutzen, 37% mehrfach pro Woche und 13% mehrfach am Tag, http://de.statista.com/statistik/daten/studie/219718/umfrage/haeufigkeit-der-nutzung-von-ausgewaehlten-sozialen-netzwerken/.

29 https://www.bitkom.org/Publikationen/2013/Studien/Soziale-Netzwerke-dritte-erweiterte-Studie/SozialeNetzwerke-2013.pdf, S. 11.

30 https://www.bitkom.org/Publikationen/2013/Studien/Soziale-Netzwerke-dritte-erweiterte-Studie/SozialeNetzwerke-2013.pdf, S. 7.

31 https://www.bitkom.org/Publikationen/2013/Studien/Soziale-Netzwerke-dritte-erweiterte-Studie/SozialeNetzwerke-2013.pdf, S. 7.

Im Folgenden soll zunächst eine abstrakte Unterscheidung der Begriffe Daten und Information erfolgen, als Grundlage der Feststellung des BVerfG, dass es „kein belangloses Datum“[32] gebe. Anschließend wird ein Überblick gegeben, welche konkreten Daten in sozialen Netzwerken anfallen und in welchem Kontext sie verwendet werden können. Hierbei liegt ein besonderes Augenmerk auf den Konsequenzen der Verwendung durch private Unternehmen; die Konsequenzen eines staatlichen Zugriffs sollen dagegen nur sehr kurz angerissen und im Übrigen der weiteren Forschung überlassen werden.

1. Unterscheidung von Informationen und Daten

Die Begriffe Informationen und Daten sind nicht synonym zu verwenden. Ihre Unterscheidung wurde insbesondere von *Albers* in aller Deutlichkeit für den juristischen Kontext formuliert[33]. In ihrem Kern beruht sie auf kommunikationstheoretischen und systemtheoretischen Überlegungen.[34]

Daten sind hiernach bloße „Zeichen“, die auf einem Datenträger festgehalten sind. Sie sind eine Informationsgrundlage, welche interpretiert und in einen Wissens- oder Bedeutungskontext eingeordnet werden muss, bevor ihr ein Inhalt entnommen werden kann.[35] Anders als Informationen sind Daten somit „vergegenständlicht“[36] und können selbstständig erfasst werden.

Informationen sind dagegen – wie *Albers* treffend formuliert hat – „Sinnelemente“: Sie stellen das Ergebnis einer Interpretationsleistung von Daten bzw. anderen Informationsgrundlagen dar.[37] Es wäre zu stark vereinfacht, davon auszugehen, dass Informationen bereits als unveränderliche Abbildungen der Realität mit einer vorgefertigten Bedeutung in Informationsgrundlagen wie Daten enthalten wären. Denn wäre dies der Fall, könnte nicht erklärt werden, warum unterschiedliche Personen unterschiedliche Informationen aus derselben Informationsgrundlage entnehmen können. Ebenso wenig könnte erklärt werden, warum im Rahmen einer Kommunikation der mitgeteilte Inhalt aus Sicht des Senders und der verstandene

---

32 BVerfGE 65, 1 (45) – Volkszählungsurteil; BVerfGE 120, 378 (399) – automatische Kennzeichenerfassung.

33 *Albers*, Rechtstheorie (33) 2002, S. 67 ff.; *dies.*¸ Informationelle Selbstbestimmung, S. 87 ff.; vgl. auch *Bäcker*, Der Staat (51) 2012, 91 (92 f.); *Trute*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 2.5, Rn. 18.

34 Vgl. die ausführlichen Nachweise bei *Albers*, Rechtstheorie (33) 2002, S. 68.

35 *Albers*, Rechtstheorie (33) 2002, S.74 f.

36 *Albers*, Rechtstheorie (33) 2002, S. 75; vgl. auch *Trute*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 2.5, Rn. 17.

37 *Albers*, Rechtstheorie (33) 2002, S. 71 ff., 74; vgl. auch *Trute*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 2.5, Rn. 18; *Hill*, DÖV 2014, 213 (218); *Bäcker*, Der Staat (51) 2012, 91 (92).

Inhalt aus Sicht des Empfängers auseinanderfallen können.[38] Informationen unterscheiden sich von Erfindungen und Illusionen auf der anderen Seite dadurch, dass sich ihr verstandener Inhalt auf real existierende Gegebenheiten oder Gegenstände bezieht und diesen auch zugeordnet wird.[39]

Informationsgrundlagen müssen also von dem Empfänger in einen Wissenskontext gesetzt und durch Interpretation verstanden werden, um eine Informationen zu erzeugen: „Informationen werden erst mit der eigenständigen Leistung des Verstehens vollendet."[40] Sie „bezeichnen weder die isolierte Aussage eines Datums noch allein dessen Interpretation, sondern das, was als Aussage eines Datums mit Hilfe einer Interpretationsleistung ermittelt wird."[41] Für die informationelle Selbstbestimmung ist dies insbesondere deshalb von Relevanz, weil es auch bedeutet, dass personenbezogene Daten und die aus ihnen ableitbaren Informationen einer einzelnen Person nicht im Sinne eines eigentumsähnlichen Rechts zugeordnet werden können. Vielmehr entstehen sie oft erst durch die Deutung anderer Personen und bewegen sich daher in einem kommunikativen, gemeinschaftlichen Kontext.[42]

Je nach Wissenshintergrund der interpretierenden Person und je nach Verwendungskontext können somit den gleichen Daten unterschiedliche Informationen entnommen werden. Durch eine lange (teilweise sogar unbegrenzte) Speicherfrist können die Daten immer wieder als Anknüpfungspunkt für die Informationsgewinnung verwendet werden und in einem anderen sachlichen oder zeitlichen Kontext betrachtet werden. Die so gewonnenen Informationen können ebenfalls in Datenform gespeichert und als neue Informationsgrundlagen für weitere Vernetzung und Analyse und damit zur Generierung von noch mehr Informationen verwandt werden.[43] Im Ergebnis handelt es sich bei diesen von *Albers* beschriebenen Zusammenhängen

---

38 *Albers*, Rechtstheorie (33) 2002, S. 69.

39 *Albers*, Rechtstheorie (33) 2002, S. 70.

40 *Albers*, Rechtstheorie (33) 2002, S. 69.

41 *Albers*, Rechtstheorie (33) 2002, S. 71; vgl. auch *Trute*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 2.5, Rn. 18.

42 *Hornung/Goeble*, CR 2015, 265 (268); *Trute*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 2.5, Rn. 19; *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 40; *Sandfuchs*, Privatheit wider Willen, S. 157 f. m.w.N.; *Buchholtz*, AöR 2015, 121 (136); vgl. auch schon BVerfGE, 65, 1, 44 – Volkszählungsurteil; *Bäcker*, Der Staat (51) 2012, 91 (92 f.). Freilich wird von einigen Autoren – insbesondere im US-amerikanischen Diskurs – unter dem Stichwort der Ökonomisierung von Daten auch eine eigentumsähnliche Zuordnung diskutiert. Insbesondere angesichts des kommunikativen und interpretatorischen Kontextes ist dies indes nicht überzeugend; vgl. für eine ausführliche Darstellung *Mayer-Schönberger*, Informationsrecht als Gestaltungsaufgabe, in: FS Druey, S. 860 ff. Vgl. auch noch vertieft zur informationellen Selbstbestimmung unten unter D.III.4.a).

43 *Albers*, Rechtstheorie (33) 2002, S. 75; *dies.*, Informationelle Selbstbestimmung, S. 96 ff.; vgl. auch *Greve*, Drittwirkung, in: FS Kloepfer, S. 670; *Bäcker*, Der Staat (51) 2012, 91 (93); zu entsprechenden konkreten Verwendungsmöglichkeiten der Daten, die durch soziale Netzwerke gewonnen werden können, ausführlich unter B.II.3.

zwischen Datenspeicherung und Informationsgewinnung also um einen sich selbst exponentiell verstärkenden Prozess: Je mehr Daten gespeichert werden, desto mehr Informationen können gebildet und ihrerseits wieder in Datenform festgehalten werden, um als Ausgangspunkt für weitere Informationsgewinnung zu dienen. Schon alleine deswegen ist es also angemessen und notwendig, den Schutz informationeller Selbstbestimmung bereits auf der Ebene der Daten ansetzen zu lassen.[44]

Die Wissens- und Kontextabhängigkeit von Informationen führt dazu, dass die Gewinnung von Informationen aus Daten ein Prozess ist. Informationsgewinnung hat insofern nicht nur eine Wissensdimension, sondern auch eine „Prozessdimension".[45] Die Information wird aus einem ständigen Abgleich mit bereits bekanntem Wissen gewonnen. Je größer hierbei das Hintergrundwissen ist bzw. je mehr verwandte Daten zur Interpretation der Informationsgrundlagen herangezogen werden können, desto aussagekräftiger sind die Informationen, die sich gewinnen lassen.

Als Konsequenz kann jedes Datum zu einem Puzzlestein in einem größeren Bild werden und einen entscheidenden Aussagegehalt bekommen. Zudem zeigt sich das prinzipielle Problem großer Datenvernetzungen: Daten werden hierdurch in einen potentiell neuen Kontext eingeordnet und können mit einem erheblich gewachsenen Wissenshintergrund analysiert werden. Dies bedeutet neue Interpretationsmöglichkeiten und damit neue Informationen, die aus dem ursprünglichen, individuellen Datum isoliert nicht hätten gewonnen werden können. Das Konzept von „Big Data" greift diesen Mechanismus in der Hoffnung auf, aus vorhandenen Daten vollkommen neue Informationen zu generieren.[46] Durch dieses „Data Mining" kann das wirtschaftliche Potential, das hinter der Vernetzung von Daten zur Informationsgewinnung steht, aktiviert werden, indem u.a. aus den unverbundenen und teilweise belanglosen Daten in sozialen Netzwerken ausführliche Persönlichkeitsprofile und weitreichende Informationen über die Nutzer gebildet werden.[47] Dieses Analysepotential soll im Folgenden ausführlicher beleuchtet werden.

---

44 *Greve*, Drittwirkung, in: FS Kloepfer, S. 670; vgl. auch *Mayer-Schönberger*, Die Tugend des Vergessens, S. 104 ff., 160 ff.; *Boehme-Neßler*, DVBl. 2015, 1282 (1283 f.).

45 *Albers*, Rechtstheorie (33) 2002, S. 69 ff.

46 *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 14 ff.; *Hackenberg*, in Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 16.7, Rn. 4 ff.

47 Ausführlich: *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 16 ff. m.w.N.; *Hackenberg*, in Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 16.7, Rn. 8; hierzu ausführlich insbesondere unter B.II.3.b)bb).

2. Anfallende Daten

Um sich der Thematik einer effektiven datenschutzrechtlichen Regulierung sozialer Netzwerke zu nähern, ist es zunächst notwendig, einen Überblick darüber zu gewinnen, welche unterschiedlichen Daten im Zusammenhang mit der Nutzung von sozialen Netzwerken erzeugt und verwendet werden.[48] Die Unterscheidung ist insbesondere deshalb von Nöten, weil die verschiedenen Datenarten ein unterschiedliches Gefährdungspotential für die informationelle Selbstbestimmung der Nutzer aufweisen und ihre Erhebung und Verwendung unterschiedlich sichtbar und kontrollierbar für den einzelnen Nutzer erfolgt.

Die anfallenden Daten können unterschiedlich systematisiert werden. Beispielsweise kann unterschieden werden zwischen „statischen" Profilinhalten, die von den Nutzern in ihre Profile eingetragen werden, und „dynamischen" Inhalten, welche insbesondere durch die Interaktion mit integrierten Angeboten anderer Nutzer entstehen.[49] Eine differenziertere Betrachtung unterteilt die Datenarten in vier unterschiedliche Kategorien: Vom Nutzer selbst publizierte „Profil- und Statusdaten", „Inhaltsdaten der Kommunikation", „Verkehrsdaten der Kommunikation" und „Nutzungs- und Reichenweitendaten".[50] Diese Betrachtungsweise kommt der Kategorisierung der deutschen Datenschutzgesetze in Verkehrs-, Bestands-, Nutzungs- und Inhaltsdaten im TKG, im TMG und implizit im BDSG bereits sehr nahe. Die entsprechende rechtliche Einordnung bestimmt maßgeblich die materielle Anwendbarkeit der jeweiligen Normen. Wenngleich die Differenzierung nach der in Zukunft geltenden DS-GVO formal nicht mehr geboten ist – angesichts der Reduzierung der bisherigen bereichsspezifischen Erlaubnistatbestände auf den Art. 6 DS-GVO – bietet sie doch zumindest als Fallgruppenbildung eine Chance für dogmatische Klarheit und soll hier daher unten unter C.III. unternommen werden.

Vor weiteren rechtlichen Betrachtungen sollen die anfallenden Daten nun zunächst kurz in ihrer funktionellen Bedeutung dargestellt werden. Hierbei soll zwischen Daten der Nutzung sozialer Netzwerke „im engeren Sinne", und solchen, die deutlich über diese Nutzung hinausgehen können – also insbesondere Reichweitendaten –, unterschieden werden. Dies erscheint

---

48 Der Verein Europe vs. Facebook, dessen Sammelklage vor dem EuGH zuletzt das Safe-Harbor-Abkommen mit den USA zu Fall brachte (EuGH, Rs. C-362/14, ZD 2015, 549 ff.), weist darauf hin, dass Facebook insgesamt über 80 verschiedene Gruppen von Daten speichert, vgl. http://www.europe-v-facebook.org/DE/Datenbestand/datenbestand.html; instruktiv zum exponentiell erhöhten Datenaufkommen im digitalen Zeitalter, auch über soziale Netzwerke hinaus: *Mayer-Schönberger*, Die Tugend des Vergessens, S. 66 ff.

49 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 50.

50 *Karg/Fahl*, K&R 2011, 453 (455).

erkenntnisversprechend, weil anhand dieser Linie wichtige Regulierungsentscheidungen verlaufen können: Insbesondere für Daten, deren Erhebung für die Nutzung des sozialen Netzwerks im engeren Sinne nicht erforderlich ist, können weit restriktivere Regelungen erlassen werden. Darüber hinaus nimmt die bewusste Kontrolle der Nutzer über die Datenerhebung und -verwendung ab, je weiter diese von ihren eigentlichen Nutzungsabsichten entfernt sind. Auch insoweit können höhere Anforderungen an die Erfüllung der staatlichen Schutzpflicht zur Gewährleistung der informationellen Selbstbestimmung der Nutzer[51] bestehen.

a) Daten der Nutzung „im engeren Sinne"

Den Daten der Nutzung im engeren Sinne unterfallen jene Daten, die Nutzer bewusst in sozialen Netzwerken preisgeben, und die im Rahmen der Kommunikation mit anderen Nutzern anfallen.

Diese umfassen insbesondere die „Profil- und Statusdaten"[52], die von Nutzern in ihrem Profil veröffentlicht werden können, beispielsweise der Name, das Alter, das Geschlecht, das Herkunftsland sowie die Interessen, Hobbies und Freunde, aber auch Angaben zu kürzlichen Aktivitäten. Hiervon zu unterscheiden sind die bei der Registrierung anzugebenden Daten, insb. die Emailadresse, das Passwort und ggf. der Name, das Geburtsdatum und die Anschrift, welche nicht für andere Nutzer, sondern nur für den Anbieter des sozialen Netzwerks verfügbar sind.

Ebenfalls in diese Kategorie fallen „Inhaltsdaten der Kommunikation".[53] Soziale Netzwerke bieten ihren Nutzern vielfältige Möglichkeiten, um Nachrichten auszutauschen, etwa in offenen Gruppen oder Foren, per privater Nachricht oder per Pinnwand-Post. Soweit die Nachrichten in öffentlich zugänglichen Gruppen gepostet werden, sind sie veröffentlichten Profilinformationen vergleichbar.[54] Soweit es sich dagegen um privat ausgetauschte Nachrichten handelt, ähneln sie funktionell einer Email.[55] Ein entscheidender Unterschied zur

---

51 Instruktiv zur insoweit bestehenden staatlichen Schutzplicht: *Trute*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 2.5, Rn. 24; *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 3 f., 36; *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 585 ff.; *Greve*, Drittwirkung, in: FS Kloepfer, S. 671 ff.; *Hoffmann-Riem*, AöR 1998, 513 (522 ff.); vgl. auch BVerfGE 117, 202 (227 f.), Rn. 62 f. – Vaterschaftstest; BVerfGK 9 353 (358 f.) - Schweigepflichtentbindung; *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 189; *Kühling*, Die Verwaltung (44) 2011, 525 (551).

52 *Karg/Fahl*, K&R 2011, 453 (455).

53 *Karg/Fahl*, K&R 2011, 453 (455).

54 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 28; *Piltz*, Soziale Netzwerke, S. 20 f.; *Karg/Fahl*, K&R 2011, 453 (455).

55 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 27; *Karg/Fahl*, K&R 2011, 453 (455); für technische Abweichungen und hieraus resultierende mögliche rechtliche Konsequenzen vgl. *Schneider*, ZD 2014, 231 (232 ff.).

Email ist indes, dass die Nachrichten dauerhaft auf den Servern des sozialen Netzwerks gespeichert werden, mithin also immer mindestens drei Personen an der Kommunikation beteiligt sind, nämlich die beiden Nutzer und der Anbieter des sozialen Netzwerks. Zudem dienen die sozialen Netzwerke nicht ausschließlich der Übertragung von technischen Signalen, so dass sie jedenfalls nicht überwiegend als Telekommunkationsdienst im Sinne des TKG einzustufen sind.[56] Hieraus ergibt sich die Frage, inwieweit das Fernmeldegeheimnis auch gegen den Anbieter des sozialen Netzwerks wirkt und ob die Nutzer tatsächlich darauf vertrauen dürfen, dass dieser die Nachrichten nicht mitliest und nicht analysiert.[57] Facebook hat gegenüber dem irischen Datenschutzbeauftragten versichert, dass es keine Auswertung der privaten Nachrichten seiner Nutzer zu Werbezwecken vornimmt. Eine Überprüfung dieser Zusicherung erfolgte allerdings nicht.[58]

Einen Graubereich beschreiten in dieser Abgrenzung die „Verkehrsdaten der Kommunikation“[59] innerhalb des Netzwerks, also „sämtliche Angaben über die Umstände der Kommunikation“[60], sowie allgemeine Nutzungsdaten über die An- und Abmeldung im sozialen Netzwerk. Bei ihnen handelt es sich zum einen um die aus den Diskussionen über die Vorratsdatenspeicherung hinlänglich bekannten Metadaten, also Angaben über Beginn und Ende einer Kommunikation und die hieran beteiligten Personen sowie Protokolldaten über die An- und Abmeldung bei dem sozialen Netzwerk durch den individuellen Nutzer. Zum anderen können sie aber auch Formen gleichsam nonverbaler Kommunikation umfassen, wie etwa die Betätigung des Like-Buttons bei Facebook oder das „Anstupsen“, bzw. „Gruscheln“ bei MeinVZ und StudiVZ.[61] Die Bezeichnung als nonverbale Kommunikation folgt daraus, dass ein Nutzer eine bestimmte Haltung zu einem anderen Nutzer oder einem Thema zu erkennen, ohne sich explizit sprachlich zu äußern.

Diese Daten liegen deshalb in einem Graubereich, weil den Nutzern formal betrachtet durchaus ein erheblicher Einfluss auf ihre Erhebung zukommt, indem sie sich aktiv für einen bestimmten Kommunikationsumfang entscheiden. Faktisch dürfte aber vielen nicht bewusst sein, dass diese Daten umfassend gespeichert werden und somit auch eine umfassende Analyse des

---

56 Hierzu noch ausführlich unten unter C.III.

57 Instruktiv für mit Chats in sozialen Netzwerken vergleichbare Instant Messenger *Schneider*, ZD 2014, 231 (234 ff., 237); vgl. auch BVerfG, DÖV 2009, 770 (770) – Email-Beschlagnahme; ausführlich noch unten unter C.III.1.

58 *Irish Data Protection Commissioner*, Report of Re-Audit, 21.9.2012, S. 18.

59 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 50; *Karg/Fahl*, K&R 2011, 453 (455).

60 *Karg/Fahl*, K&R 2011, 453 (455).

61 So bereits *Karg/Fahl*, K&R 2011, 453 (455).

Kommunikationsverhaltens innerhalb des Netzwerks erlauben.[62] Dass die Gesamtheit dieser Daten schnell zu erstaunlich großen Datenmassen führen kann, zeigt der Fall des österreichischen Jurastudenten Max Schremm, welcher nach wiederholter Geltendmachung seiner Auskunftsrechte gegenüber Facebook ein PDF Dokument im Umfang von 1222 DinA4 Seiten, zugesandt bekam.[63]

Als technische Kehrseite der Inhaltsdaten der Kommunikation ist die Erhebung dieser Daten freilich unvermeidbar und das eingeschränkte Bewusstsein der Nutzer zumindest teilweise auch einem gewissen Desinteresse an der Auseinandersetzung mit technischen Fragen geschuldet. An ihr zeigt sich auch, dass eine Abgrenzung anhand der durchschnittlichen Kontrolle des Nutzers nur für eine erste, überblicksartige Faustformel, nicht aber für eine detaillierte rechtliche Einordnung geeignet ist.

b) Nutzungs- und Reichweitendaten

In einem fließenden Übergang zu den Verkehrsdaten der Kommunikation liegen die Daten über die An- und Abmeldung im sozialen Netzwerk, verbunden mit den technischen Identifikationsmechanismen wie beispielsweise der IP-Adresse. In der Kategorisierung von *Karg* und *Fahl* handelt es sich zunächst um „sämtliche Informationen, die Auskunft über die Häufigkeit, den Umfang und die Art der Nutzung des Netzwerkes ergeben“[64]. Soweit es hierbei um Merkmale zur Identifikation eines Nutzers geht, sowie Angaben, die zur Ermöglichung der Inanspruchnahme des Dienstes erforderlich sind, besteht eine weitgehende Übereinstimmung mit dem rechtlichen Begriff der Nutzungsdaten aus § 15 TMG.[65]

Neben Daten über An- und Abmeldezeitpunkt wird auch gespeichert, wie lange sich ein Nutzer auf anderen Profilen bzw. im Fall von Facebook auch auf Fanpages aufgehalten hat.[66] Von besonderer Bedeutung ist aber, dass im Rahmen der sogenannten Reichweitenanalyse zahlreiche Daten über die Nutzung sonstiger Internetangebote erhoben werden. Insbesondere Facebook nutzt die im Zusammenhang mit dem sozialen Netzwerk gewonnenen Identifikationsmöglichkeiten, um Nutzer in weiten Teilen des gesamten Internets zu verfolgen

---

62 *Karg/Fahl*, K&R 2011, 453 (455); *Maisch*, Informationelle Selbstbestimmung, S. 220, der auch darauf hinweist, dass sich sogar aus Löschungswünschen von Nutzern relevante Informationen für Facebook ergeben, da Facebook Aufschluss darüber erhält, welche Daten ein Nutzer nicht mehr verfügbar wissen will bzw. mit welchen Personen ein Nutzer beispielsweise nicht mehr befreundet sein will.

63 http://www.europe-v-facebook.org/sk/sk.pdf, S. 29, Rn. 159; *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner, S. 423.

64 *Karg/Fahl*, K&R 2011, 453 (455).

65 Ausführlich zum rechtlichen Begriff der Nutzungsdaten unten unter C.III.3.

66 Vgl. *Karg/Fahl*, K&R 2011, 453 (455).

und Daten unter anderem über individuelle Interessen, die sozio-ökonomische Stellung und das Konsumverhalten zu erheben.[67] Die Nutzer werden hierüber weder ausdrücklich informiert, noch können sie Facebook gegenüber widersprechen. Es handelt sich damit um eine vom Nutzer weitgehend unbemerkte, häufig nicht bewusst gebilligte Form der Datenerhebung, die besonders fruchtbare Informationsgrundlagen hervorbringt und Anbietern sozialer Netzwerke wie Facebook daher erhebliche Rückschlüsse auf den einzelnen Nutzer ermöglicht.

Im Folgenden sollen die im Rahmen der Reichweitenanalyse relevanten Tracking-Methoden dargestellt und damit die Art der erhobenen Daten noch weiter präzisiert werden.

aa) Cookies und Social PlugIns

Eine zentrale Technik zur Verfolgung des Nutzerverhaltens im Internet sind sogenannte „Cookies".[68] Hierbei handelt es sich im Prinzip um kleine Textdateien, die auf dem Endgerät des Nutzers abgelegt werden. Sie archivieren Informationen über das Internetverhalten des Nutzers und zuvor besuchte Webseiten. Diese Informationen versenden sie auf automatische Abfragen hin an den Verantwortlichen, der den Cookie gesetzt hat – beispielsweise facebook.com – ohne dass dies für den Nutzer direkt erkennbar ist. Sie ermöglichen entsprechend dem Empfänger des Cookies, das Endgerät und damit mit relativ hoher Wahrscheinlichkeit seinen Nutzer zu identifizieren. Bei Cookies handelt sich daher im Grundsatz um personenbezogene Daten.[69]

Cookies müssen nicht zwingend von dem Anbieter der Webseite gesetzt werden, auf der sich ein Nutzer gerade aufhält (sog. „First-Party-Cookies"). Sie können vielmehr auch von Drittanbietern und damit anderen datenschutzrechtlich Verantwortlichen über diese Webseite

---

67 *Karg/Fahl*, K&R 2011, 453 (455); ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 23; hierzu ausführlicher sogleich unter B.II.3.

68 Für eine ausführliche Definition von Cookies vgl. http://tools.ietf.org/html/rfc6265; *Spindler/Nink*, in: Spindler/Schuster, § 11 TMG, Rn. 21 und § 13 TMG, Rn. 5; Art. 29 DatSchGruppe, Stellungnahme 4/2012, WP 194, S. 2 ff.; *Dieterich*, ZD 2015, 199 (199); vgl. auch schon Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 6 ff.

69 *Spindler/Nink*, in: Spindler/Schuster, § 11 TMG, Rn. 21; *Riefa/Markou*, Online Marketing, in: Savin/Trzaskowski (Hrsg.) Research Handbook on EU Internet Law, S. 397 f., 401; a.A. *Spindler*, GRUR-Beilage 2014, 101 (105), solange keine ergänzenden identifizierenden Daten für die verantwortliche Stelle verfügbar sind.

gesetzt werden (sog. „Third-Party-Cookies“).[70] Zudem kann man Cookies danach differenzieren, ob sie nur für die Dauer gespeichert werden, in welcher der Browser geöffnet ist, und anschließend gelöscht werden (sog. „Sitzungs-“ oder „Session-Cookies“) oder ob sie bis zu einem festgelegten Ablaufdatum auf dem Endgerät des Nutzers gespeichert bleiben und während dieser Zeit bei jedem Zugriff auf die zugehörige Webseite Informationen senden (sog. „persistente Cookies“).[71]

Eine wesentliche Funktion von Cookies ist, dass sie individuelle Nutzerpräferenzen speichern und an besuchte Webseiten übermitteln. Dies kann die Internetnutzung beschleunigen, indem beispielsweise Angaben über die optimale Darstellungsweise auf dem Endgerät vorab übermittelt oder Passwörter zwischengespeichert werden. Viele Internetdienste könnten ohne Cookies nicht funktionieren, da eine kontinuierliche Identifizierung des Nutzers nicht möglich wäre. Insbesondere im Bereich des eCommerce könnte beispielsweise nicht ohne Weiteres sichergestellt werden, dass der Nutzer, der am Ende auf „Bezahlen“ klickt, auch derjenige ist, der zuvor die Waren in den Warenkorb gelegt hat und er entsprechend die Waren erhält, die er haben wollte. Es wäre daher sicherlich verfehlt, Cookies grundsätzlich als schädlich zu betrachten.[72] Vielmehr ist sogar allgemein anerkannt, dass ihr Einsatz gemäß Art. 5 Abs. 3 S. 2 Var. 2 der Richtlinie 2002/58/EG (EK-DSRL)[73] in der Fassung der Richtlinie 2009/136/EG[74] unter bestimmten Voraussetzungen sogar von einer Einwilligungspflicht des Nutzers befreit sein kann.[75]

Die zweite zentrale Technik zur Verfolgung von Nutzern im Internet sind sogenannte Social PlugIns. Social PlugIns sind Dienstelemente, die auf Webseiten eingebunden werden können

---

70 Art. 29 DatSchGruppe, Stellungnahme 4/2012, WP 194, S. 5. Aus „Browsersicht“ könnte der Begriff des „Third-Party-Cookies“ freilich auch weiter verstanden werden, so dass es sich nur um einen Cookie handeln muss, der von einer Webseite gesetzt wurde, deren Domäne (URL) nicht identisch ist mit der Domäne der in der Adresszeile des Browsers angezeigten Webseite. Es wäre hingegen nicht erforderlich, dass er auch von Dritten im Sinne von Art. 2 lit f.) DSRL gesetzt wurde, es sich also um einen vom Betreiber der besuchten Webseite verschiedenen für die Verarbeitung Verantwortlichen handelt. Ist Übereinstimmung mit der Stellungnahme der Art. 29 DatSchGruppe (a.a.O.) soll hier indes von dem engeren Begriff ausgegangen werden.

71 Art. 29 DatSchGruppe, Stellungnahme 4/2012, WP 194, S. 4.

72 *Spindler/Nink*, in: Spindler/Schuster, § 11 TMG, Rn. 21; Art. 29 DatSchGruppe, Stellungnahme 4/2012, WP 194, S. 7 f.

73 Richtlinie 2002/58/EG des europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

74 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst uA cnd Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

75 Für eine ausführliche Analyse siehe Art. 29 DatSchGruppe, Stellungnahme 4/2012, WP 194, S. 2 ff.; rt. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 9 ff.; *Zscherpe*, in: Taeger/Gabel, § 15 TMG, Rn. 37.

und die es ermöglichen, einzelne Funktionen der zugehörigen sozialen Netzwerksplattform zu nutzen, beispielsweise fremde Zeitschriften- oder Zeitungsartikel im Netzwerk zu teilen.[76] Sie sind mittlerweile verhältnismäßig weit im Internet verbreitet. Insbesondere der bekannte „Like-Button" Facebooks ist aktuell auf fast zwei Millionen Webseiten integriert, sowohl auf zahlreichen privaten als auch staatlichen Angeboten.[77] Weitere Beispiele sind der +1 Button von Google Plus oder der Tweet bzw. Follow Button von Twitter. Auch die anderen sozialen Netzwerke bieten in aller Regel vergleichbare Social PlugIns an[78], u.a. Xing, LinkedIn, Pinterest und Tumblr.

Cookies können so programmiert werden, dass sie mit bestimmten Social PlugIns bzw. den hinter ihn stehenden sozialen Netzwerken kommunizieren. Hieraus ergibt sich ihr enormes Überwachungs- und Verfolgungspotential: Solange sich ein bestimmter Cookie auf einem Endgerät eines Nutzers befindet, sendet dieser beim Besuchen jeder Webseite mit dem korrespondierenden Social PlugIn eine Information an den Anbieter des sozialen Netzwerks, dass dieses Endgerät – und damit wahrscheinlich der Nutzer – diese Webseite aufgerufen hat.[79] Angesichts der weiten Verbreitung insbesondere des Like-Buttons ermöglicht dies den

---

76 Ausführlich: ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 7 f.; *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 89 f.

77 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 90; http://trends.builtwith.com/widgets/Facebook-Like. Die tatsächliche Zahl der Like-Buttons könnte noch deutlich höher liegen. So war der Like-Button nach der zitierten Studie der KU Leuven am 21.März.2015 noch auf mehr als 13 Millionen Seiten laut der ebenfalls soeben zitierten Statistik integriert. Wie der Grafik auf der Internetseite zu entnehmen ist, fand im März 2015 ein Absturz der integrierten Like-Buttons insbesondere auf den meistgenutzten Internetseiten statt. Während ein plötzliches synchrones Entfernen des Like-Buttons auf über 150.000 sehr populären Webseiten und zahlreichen weiteren zwar möglich ist, bietet sich auch eine andere Interpretation an: Bis März 2015 bot Facebook vier unterschiedliche Möglichkeiten der Integration des Like-Buttons in andere Webseiten an, von denen eine Variante dazu führte, dass nicht bereits bei Aufruf der Webseite automatisch Daten an Facebook übertragen wurden. Diese Option wird seitdem nicht mehr von Facebook angeboten, lässt sich aber über Drittanbieter immer noch verwirklichen, vgl. *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 99, sowie ausführlich unten unter D.I.3.d). Es ist daher jedenfalls denkbar, dass diese Veränderung die Statistik verzerrt, indem beispielsweise über Drittanbieter integrierte Like-Buttons nicht ordnungsgemäß erfasst werden. Dafür spricht auch, dass seit der dramatischen Abnahme von integrierten Like-Buttons im März 2015 eine relativ stabile Verwendung mit teilweise sogar positivem Zuwachs beobachten ist. Dies ist aber letztlich rein spekulativ und kann im Rahmen dieser Arbeit nicht überprüft werden.

78 Vgl. *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 89; *Voigt/Alich*, NJW 2011, 3541 (3541 f.).

79 *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1, Rn. 47; *Karg/Thomsen*, DuD 2012, 729 (731); *Pariser*, Filter Bubble, S. 41 f. Diese Funktion des Social PlugIns lässt sich allerdings seitens des Webseitenbetreibers unterbinden, wenn er dieses technisch so auf seiner Webseite einbindet, dass erst beim Anklicken des Social Plug Ins diese Daten gesendet werden, sog. 2-Klick-Lösung.

Anbietern von sozialen Netzwerken ein weitreichendes Tracking von ihren Nutzern, teilweise sogar auch von Nichtnutzern, im gesamten Internet.[80]

Auch Facebook verwendet selbstverständlich Cookies, da sein Diensteangebot sonst technisch nicht möglich wäre. Die datenschutzrechtlich relevantesten Cookies sind „datr" (Browser-ID), „c_user" (Facebook ID) und „fr" (verschlüsselte Facebook und Browser ID).[81] Der c_user-Cookie und der fr-Cookie werden jeweils beim Login eines Nutzers gesetzt und ermöglichen insbesondere eine Identifizierung und die Ermöglichung einer einheitlichen Sitzung. Einige dieser Cookies können darüber hinaus mit Social-PlugIns kommunizieren und detaillierte Informationen über die Aktivitäten eines Nutzers auf Drittanbieter-Webseiten mit Social PlugIns senden.[82] Solange ein Nutzer diese Cookies nicht von seinem Endgerät gelöscht hat – im Zweifel manuell – ist sein Verhalten im Internet damit für Facebook weitgehend nachvollziehbar und verfolgbar. Dies bestätigt Facebook im Rahmen seiner Bestimmungen zur Verwendung von Cookies, in denen es heißt:

> *„Wir verwenden Cookies, wenn du ein Facebook-Konto hast, die Facebook-Dienste, einschließlich unserer Webseite und Apps, nutzt (gleichgültig, ob du registriert oder angemeldet bist) oder andere Webseiten und Apps besuchst, die die Facebook-Dienste nutzen (einschließlich der „Gefällt mir"-Schaltfläche bzw. unserer Werbefunktionen). […] Wir verwenden Cookies als Unterstützung, um Werbeanzeigen für Unternehmen und sonstige Organisationen denjenigen Personen anzuzeigen, die sich möglicherweise für die von ihnen hervorgehobenen Produkte, Dienstleistungen bzw. wohltätigen Zwecke interessieren. Beispiel: Mithilfe von Cookies können wir Werbeanzeigen denjenigen Personen anzeigen, die bereits zuvor die Webseite eines Unternehmens besucht, seine Produkte gekauft oder seine Apps verwendet haben."*[83]

Von besonderer datenschutzrechtlicher Bedeutung ist der datr-Cookie. Dieser ist ein persistenter Cookie, der bis zu zwei Jahre lang gültig ist und gespeichert bleibt, sofern er nicht aktiv von dem Nutzer des Endgeräts gelöscht wird. In diesem Zeitraum sendet er bei jedem Aufruf der Webschnittstelle facebook.com die durch die Cookies gesammelten Inhalte an

---

80 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 89 f.; *Martini/Fritzsche*, VerwArch (104) 2013, 449 (455); *Riefa/Markou*, Online Marketing, in: Savin/Trzaskowski (Hrsg.) Research Handbook on EU Internet Law, S. 384; *Karg/Thomsen*, DuD 2012, 729 (730 f.); ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S.17 f.

81 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 89 ff.; Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 16 ff.; *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 175; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 7 f.

82 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 89 ff.; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 7 ff.; *Karg/Fahl*, K&R 2011, 453 (454).

83 https://www.facebook.com/policies/cookies/ (Stand 20. März 2017).

Facebook.[84] Zu dem Aufruf der Webschnittstelle kann es beim Besuch von Webseiten mit integriertem Like-Button kommen, wenn der Like-Button entsprechend eingebunden und programmiert ist. Während es technische Möglichkeiten für den Webseitenbetreiber gibt, um diesen automatischen Aufruf zu unterbinden, führt jedenfalls die von Facebook standardmäßig angebotene technische Einbindung stets zu einem solchen automatischen Aufruf.[85] Zwar sendet der datr-Cookie keine detaillierten Informationen über die genauen Aktivitäten auf der Drittanbieter-Webseite; aber auch aus dem bloßen Aufruf einer Webseite lassen sich bereits Rückschlüsse auf die Anliegen der Nutzer ziehen. So ist relativ klar, dass eine Person, die eine Seite zum Vergleich von Preisen für Flugtickets aufruft, eine Reise plant und kostenbewusst vorgehen möchte. Ebenso ist naheliegend, dass eine Person, die eine Online-Apotheke besucht, sich für Medikamente interessiert und eine Person, die Nachrichtenseiten aufruft, sich informieren möchte.

Der datr-Cookie wird automatisch gesetzt, wenn ein Endgerät in Kontakt mit der Domain facebook.com kommt. Es ist nicht erforderlich, sich bei Facebook zu registrieren oder anzumelden. Er wird damit auch für Nichtnutzer gesetzt und ermöglicht ihnen gegenüber die soeben beschriebene Verfolgung.[86] Facebook gibt an, dass dies aus Sicherheitsgründen erforderlich sei, unter anderem um Bot-Netze zu enttarnen und Distributed Denial of Services (DDoS) Attacken zu unterbinden.[87] Mit dieser Begründung hat sich der irische Datenschutzbeauftragte in seinem Audit zufrieden gegeben und die resultierende Verfolgung

---

84 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 89; Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 16 f.; *Karg/Thomsen*, DuD 2012, 729 (730 ff.); *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 172 ff.; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 7 f.; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 7 f.

85 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 99; vgl. auch die Bestimmungen zur Verwendung von Cookies von Facebook: „Wir können Cookies auf deinem Computer oder Gerät platzieren und so Informationen erhalten, die in den Cookies gespeichert werden, wenn du folgende Dienste nutzt bzw. besuchst: […] Dienste, die von anderen Unternehmen bereitgestellt werden, die die Facebook-Dienste nutzen (z. B. Unternehmen, die die „Gefällt mir"-Schaltfläche oder die Werbedienste von Facebook in ihre Webseiten und Apps integrieren).", https://www.facebook.com/policies/cookies/ (Stand 30. März 2017); zu den technischen Details und der daraus resultierenden möglichen Verantwortlichkeit der Webseitenbetreiber ausführlich unten unter D.I.3.d).

86 *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 82, 173 ff.; *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 97; Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 18 f.; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 6 ff.; *Karg/Thomsen*, DuD 2012, 729 (730 f.); AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 7.

87 *Beckendorf*, MMR-Aktuell 2015, 374256; vgl. auch *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 176.

von Nichtnutzern im Internet für zulässig erachtet.[88] Nach hier vertretender und weithin geteilter Ansicht trifft dies nicht zu.[89] Vielmehr ist die Verfolgung von Nichtnutzern mit dem datr-Cookie in dem aktuellen Umfang datenschutzrechtlich nicht legitimiert und als rechtswidrig einzustufen. Um die in diesem Abschnitt vorgenommene Problemanalyse nicht zu überladen, sei indes für die ausführliche rechtliche Analyse nach unten verwiesen.[90]

Im Zusammenspiel von identifizierenden Cookies und Social PlugIns ergeben sich für die Anbieter sozialer Netzwerke somit erhebliche Möglichkeiten, Nutzer und teilweise sogar Nichtnutzer weit über das soziale Netzwerk hinaus im gesamten Internet zu verfolgen und damit Daten über ihr Verhalten zu sammeln.

bb) Browser Fingerprinting

Eine neuere Form des Trackings ist das sogenannte Browser-Fingerprinting bzw. allgemeiner auch Device Fingerprinting. Moderne Browser senden eine Vielzahl an Informationen an die aufzurufende Webseite und damit ihren Betreiber, um eine optimale Darstellung der Inhalte auf der Webseite zu gewährleisten. Diese Informationen beinhalten unter anderem das Betriebssystem des Nutzers, im Browser installierte PlugIns, Art und Version des Browsers, Spracheinstellungen und verwendete Sprachen.[91] Isoliert betrachtet werden viele dieser Merkmale bei zahlreichen Browsern vorkommen. In der konkreten Zusammenstellung der Merkmale können sie jedoch zur Identifikation einzelner Nutzer genutzt werden. Diese ist dabei umso leichter möglich, je benutzerdefinierter der Browser ausgestaltet ist. Insbesondere Nutzer, die durch individuelle Modifikationen ihres Browsers sicherstellen wollen, möglichst wenig im Internet verfolgt zu werden, können somit sogar leichter identifiziert werden.[92] Inwieweit Browser-Fingerprints Personenbezug und damit datenschutzrechtliche Relevanz besitzen, ist noch nicht höchstrichterlich entschieden worden.[93] Isoliert betrachtet gibt es – anders als bei

---

88 *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 82, 173 ff.; *Irish Data Protection Commissioner*, Report of Re-Audit, 21.9.2012, S. 28.

89 So auch *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 98; Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 19 ff.; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 23 f.; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 24 f.; *Beckendorf*, MMR-Aktuell 2015, 374256.

90 Vgl. unten unter D.I.3.c)aa)i).

91 *Voigt*, Webbrowser Fingerprints, in: Taeger (Hrsg.), LaaS, Recht im Internet und Cloudzeitalter, S. 161; *Sandfuchs*, Privatheit wider Willen, S. 15 f.; *Dieterich*, ZD 2015, 199 (200); *Karg/Kühn*, ZD 2014, 285 (286 f.); Art. 29 DatSchGruppe, Stellungnahme 9/2014, WP 224, S. 6.

92 *Voigt*, Webbrowser Fingerprints, in: Taeger (Hrsg.), LaaS, Recht im Internet und Cloudzeitalter, S.162 f.

93 Vgl. instruktiv zum Streitstand die sehr ausführliche Darstellung bei *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, S. 373 ff.

IP-Adressen – keine direkte Zuordnung von Browser-Fingerprint und Nutzer. Allerdings wird der Browser-Fingerprint häufig parallel zur IP-Adresse erhoben und gespeichert. Zudem kann eine Zuordnung erfolgen, wenn sich ein Nutzer über eine Anmeldung z.B. in einem sozialen Netzwerk über diesen Browser zu erkennen gibt und dies gespeichert wird. Es ist somit regelmäßig davon auszugehen, dass die den Browser-Fingerprint erhebende Stelle Zusatzwissen hat, welches die Bestimmung der Person ermöglicht.[94] Dies ist insbesondere bei Anbietern sozialer Netzwerke der Fall. Somit ist es vorzugswürdig, den Browser-Fingerprint in der Regel als personenbezogenes Datum zu behandeln.[95]

Für Anbieter sozialer Netzwerke lassen sich Browser-Fingerprints einsetzen, um die aus Cookies und Social PlugIns gewonnenen Informationen weiter zu verfeinern und zu verifizieren, indem eine noch detaillierte Zuordnung des Nutzers vorgenommen werden kann. Browser-Fingerprinting kann zudem Selbstschutzmaßnahmen von Nutzern untergraben, die regelmäßig die Cookies löschen und daher dafür sorgen, dass diese nur begrenzte Mengen an identifizierenden Daten sammeln und speichern können. Indem sie über Browser-Fingerprinting jederzeit genau identifizierbar werden, genügt es für eine Zuordnung, verhältnismäßig inhaltsleere Cookies zu haben, die gerade erst abgelegt wurden und die eine Sendung der Informationen über ein Social PlugIn veranlassen.

cc) Integrierte Dienste und Internet.org

Über die soeben beschriebene weitreichende Verfolgung seiner Nutzer im gesamten Internet arbeitet Facebook längst an dem nächsten logischen Schritt, um noch mehr Daten über seine Nutzer zu erhalten: Die Nutzer sollen dazu angehalten werden, Facebook möglichst gar nicht mehr zu verlassen und stattdessen das Internet nur noch in Facebook integriert zu nutzen. Für Facebook beseitigt dies den zusätzlichen Aufwand, seine Nutzer umständlich auf anderen Webseiten zu verfolgen.

Bereits realisiert ist dies beispielsweise für durch Nutzer in ihr Profil eingebettete und mit ihren Freunden geteilte Youtube-Videos oder sogenannte „Instant Articles“ kooperierender Onlinemedien. Letzteren wird die Möglichkeit gegeben, ihre Artikel direkt in Facebook zu

---

94 *Voigt*, Webbrowser Fingerprints, in: Taeger (Hrsg.), LaaS, Recht im Internet und Cloudzeitalter, S. 164; *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, S. 404; *Karg/Kühn*, ZD 2014, 285 (288); *Martini/Fritzsche*, VerwArch (104) 2013, 449 (455); Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 11; Art. 29 DatSchGruppe, Stellungnahme 9/2014, WP 224, S. 6.

95 Art. 29 DatSchGruppe, Stellungnahme 9/2014, WP 224, S. 4, 7; *Dieterich*, ZD 2015, 199 (203 f.); *Karg/Kühn*, ZD 2014, 285 (288); *Martini/Fritzsche*, VerwArch (104) 2013, 449 (455).

integrieren, anstatt nur einen Link zur eigenen Seite zu posten.[96] Diese Onlinemedien verzichten hierfür auf Klicks auf ihren eigenen Webseiten, die sie eigentlich brauchen, um Geld über Onlinewerbung zu generieren. Im Gegenzug gestattet ihnen Facebook, Werbung im Umfeld ihres integrierten Artikels zu schalten. Zudem erhalten sie von Facebook demografische Daten über die Nutzer, die auf die Artikel geklickt haben und damit wichtige Informationen für ihre Marketing-Strategien.[97] Für Facebook hat es den Vorteil, dass der Nutzer direkt innerhalb des sozialen Netzwerks bleibt und ein Wechsel aus ihm heraus überflüssig erscheint.

Facebook hat zudem eine Funktion geschaffen, um Onlineshops in seinem Netzwerk direkt zu integrieren.[98] Unternehmen, die diese Möglichkeit wahrgenommen haben, scheinen bisher zwar insbesondere in Deutschland keinen allzu großen Erfolg damit gehabt zu haben, vor allem infolge einer bisher mangelnden Begeisterung der Nutzer für eine Bezahlfunktion via Facebook.[99] In dem Maße, in dem diese Skepsis abnimmt und eine Akzeptanz integrierter Onlineshops wächst, erhöht sich aber auch der direkte Zugriff Facebooks auf Daten über das Konsumverhalten seiner Nutzer, deren Wechsel auf andere Verkaufsplattformen sich gegebenenfalls erübrigt.

Medienberichten zufolge hat Facebook im April 2014 zudem in Irland eine Lizenz beantragt, um zu einem sogenannten e-Geld-Institut zu werden. Hiermit hätte Facebook das Recht, innerhalb seines Netzwerks Überweisungen von Nutzern innerhalb der EU vornehmen zu lassen.[100] Facebook könnte damit direkt nachvollziehen, welche Person einer anderen welche Menge Geld zukommen lässt und erneut einen Angriff auf etablierte Konkurrenten wie etwa PayPal in diesem Gebiet starten. Eine entsprechende Funktion in der Facebook Messenger App, die immerhin von 500 Millionen Nutzern auf Smart-Devices installiert ist, integriert sein.[101]

Fast seit Beginn von Facebook gibt es zudem die Möglichkeit, sich über integrierte Spiele und andere Apps die Zeit innerhalb des sozialen Netzwerks zu vertreiben. Auch hiermit lockt Facebook seine Nutzer fort von etablierten Webseiten, die die sogenannten Browsergames anbieten, und hinein in sein eigenes Netzwerk.

---

96 *Reuters Institute*, http://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital-News-Report-2016.pdf, S. 8; http://www.zeit.de/kultur/2015-05/instant-articles-facebook-meinungsfreiheit/komplettansicht.

97 http://www.zeit.de/kultur/2015-05/instant-articles-facebook-meinungsfreiheit/komplettansicht.

98 *Lichtnecker*, GRUR 2013, 135 (136).

99 http://www.projecter.de/blog/social-media/top-10-der-deutschen-facebook-shops.html.

100 http://www.zeit.de/digital/internet/2014-04/facebook-ueberweisungen-e-geld/komplettansicht; http://www.sueddeutsche.de/digital/lizenz-in-irland-beantragt-facebook-will-eine-bank-werden-1.1958655.

101 http://www.zeit.de/digital/internet/2015-03/facebook-messenger-bezahlen-geld.

Wohin diese Bestrebungen in letzter Konsequenz gehen können, zeigt sich an dem Projekt „Internet.org“: Mit diesem bietet Facebook in Kooperation mit Mobilfunkanbietern und Smartphone-Herstellern einen kostenlosen „Internetzugang“ in Ländern wie Indien, Tansania, Ghana und Bangladesch. Das erklärte Ziel ist, die zwei Drittel der Menschheit, die sich heute noch keinen Internetzugang leisten können, mit einem Internetzugang zu versorgen – und damit auch ihre persönlichen Daten zu erhalten. Im Rahmen des zunächst großzügig erscheinenden Angebots wird aber nur Zugang zu der Seite von Facebook sowie einigen wenigen weiteren Seiten ausgewählter Kooperationspartner gewährt. Für einen vollständigen Internetzugriff im Rahmen eines normalen Mobilfunkvertrags fallen dagegen Gebühren an, die für viele nicht finanzierbar sind.[102] Ob ein solches Angebot überhaupt rechtmäßig ist, insbesondere da es die Netzneutralität erheblich einschränken und damit wettbewerbsverzerrend wirken kann, ist bisher ungeklärt und muss der weiteren Forschung überlassen bleiben.[103] Ethisch stellt sich zudem die grundsätzliche Frage, ob ein eingeschränkter und manipulierbarer Zugriff auf kleine Teile des Internets nicht zumindest besser ist als gar keinen Zugriff zu haben. Auch die Beantwortung dieser Frage würde an dieser Stellt indes zu weit gehen.

Mit internet.org vergleichbare Entwicklungen sind in Deutschland bisher noch nicht zu beobachten. Angesichts eines verhältnismäßig gut funktionierenden Wettbewerbs unter den Anbietern eines Internetzugangs und der relativ hohen Kaufkraft in der Bevölkerung ist es auch unwahrscheinlich, dass sich ein einzelnes Unternehmen wie Facebook bereits an dieser Stelle als Monopolist etablieren könnte. Es sei allerdings kurz darauf hingewiesen, dass es in bestimmten Marktbereichen durchaus in diese Richtung gehende Ansätze gibt, beispielsweise das integrierte, kostenlose Angebot des Streaming-Dienstes Spotify bei Mobilfunkverträgen der deutschen Telekom.[104]

Durch die fortschreitende Integration verschiedenster Internetdienste in sein soziales Netzwerk schafft Facebook mithin die Voraussetzungen für eine umfassende Nutzerüberwachung, ohne hierbei noch länger auf Tracking-Methoden angewiesen zu sein. Die Nutzeraktivität verlagert sich vielmehr direkt in das soziale Netzwerk und erlaubt damit eine direkte Analyse. Eine Opt-Out Möglichkeit besteht dann nur noch in Form der vollständigen Nichtnutzung des sozialen Netzwerks und der integrierten Dienste, soweit diese exklusiv an jenes gebunden sind.

---

102 https://www.internet.org/about; http://www.zeit.de/digital/internet/2015-04/internet-org-facebook-netzneutralitaet; http://www.handelsblatt.com/unternehmen/it-medien/facebook-und-internet-org-indiens-aufstand-gegen-mark-zuckerberg/11663668-all.html.

103 Vgl. bereits in dieser Richtung kritisch, allerdings in Bezug auf Streaming-Dienste *Franke/Rogge*, VerwArch (106) 2015, 352 (356 ff.).

104 Vgl. hierzu kritisch *Franke/Rogge*, VerwArch (106) 2015, 352 (356, 366 ff.).

3. Verwendungsmöglichkeiten der Daten

Die soeben skizzierten Arten von im Zusammenhang mit sozialen Netzwerken erhobenen Daten können auf sehr unterschiedliche Weise verwendet werden. Ganz grundlegend ist zwischen der Nutzerperspektive und der Anbieterperspektive zu unterscheiden, die sehr verschiedene Zwecke mit diesen Daten verfolgen.

a) Nutzerperspektive

Die Nutzer sozialer Netzwerke veröffentlichen persönliche Daten, um sich selbst darzustellen und eine Identität gegenüber den anderen Nutzern aufzubauen und zu präsentieren.[105] Durch eine gezielte Auswahl von Interessenangaben, Fotos und Statusmeldungen haben Nutzer eine große Kontrolle darüber, wie sie sich nach außen darstellen. Gerade jüngeren Nutzern bietet die Freiheit der Profilerstellung die Möglichkeit, mit unterschiedlichen Selbst- und Fremdbildern zu experimentieren und damit ihre Identität zu finden. Dies begründet einen großen Teil des Reizes von sozialen Netzwerken speziell in jüngeren Altersgruppen.[106] Gleichzeitig verleitet diese Funktion freilich dazu, immer mehr über sich selbst auch preiszugeben, wenn man ein möglichst umfassendes Bild von sich selbst zeichnen möchte. Diese Tendenz wird von den Anbietern sozialer Netzwerke auch bewusst gefördert, indem diese durch das Design der Plattform und der Profilschablonen Nutzer ermutigen, mehr Angaben über sich selbst zu machen.[107]

In eher beruflich orientierten sozialen Netzwerken wie Xing oder LinkedIn können sich darüber hinaus Arbeitnehmer und Selbstständige gezielt mit potentiellen neuen Arbeitgebern oder Auftraggebern vernetzen. Soziale Netzwerke übernehmen hier die Funktion von Karrieremessen und bieten eine Chance zur öffentlichen Bewerbung.

Soziale Netzwerke bieten zudem umfangreiche Kommunikationsfunktionen. Sie ermöglichen ihren Nutzern, neue Interessenverwandte zu finden und mit aus der offline-Welt bekannten Personen Kontakt zu halten.[108] Die Kontakte von Nutzern und die daraus entstehenden

---

105 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 34 ff., 50 f., 131 ff.; *Lerch/Krause/Hotho/Roßnagel/ Stumme*, MMR 2010, 454 (457); *Autenrieth*, in: Neumann-Braun/Autenrieth (Hrsg.), Freundschaft und Gemeinschaft im Social Web, S. 148 f.

106 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 32 ff.

107 *Maisch*, Informationelle Selbstbestimmung, S. 169; *Martini/Fritzsche*, VerwArch 2014, 450 (453); vgl. auch *Grimmelmann*, 94 Iowa L.Rev. 1137 (1149 ff.), 2008-2009.

108 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 34 ff., 131 ff.; *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 89 f.; *Lerch/Krause/Hotho/Roßnagel/ Stumme*, MMR 2010, 454 (457).

Netzwerke bilden daher häufig real existierende „analoge“ Netzwerke nach.[109] Nutzer können sich zu Veranstaltungen verabreden und diese planen, sowie individuell oder öffentlich kommunizieren, indem private Nachrichten verschickt oder Meldungen auf der Profilseite gepostet werden. Kommunikation wird komfortabler und einfacher gestaltet, indem beispielsweise zeitversetzte Gruppenchats ohne irgendeinen Zeitaufwand eingerichtet werden können. So können auch mehrere Nutzer asynchron miteinander kommunizieren, ohne dass beispielsweise zahlreiche Emails verschickt werden müssen.

Über die Kommunikation mit Bekannten hinaus kann auch Kontakt mit zahlreichen Unternehmen oder Institutionen aufgenommen werden, die ihrerseits Profile pflegen. Im Rahmen von Facebook sind dies die sogenannten Fanpages. Unternehmen, Institutionen und Personen des öffentlichen Lebens äußern sich hier und bieten Nutzern die Möglichkeit, direkt auf Angebote oder Aussagen zu kommentieren. Teilweise sehr umfangreiche Social-Media Abteilungen kümmern sich um einen intensiven Kundenkontakt und einen direkten, zeitnahen Austausch.

Als Umkehrung der Selbstdarstellungsmöglichkeiten bieten soziale Netzwerke zuletzt die Möglichkeit, sich über andere Nutzer zu informieren. Wer mehr über eine kürzliche neue Bekanntschaft erfahren möchte, kann dies gegebenenfalls über das Profil dieser Person tun. Die dort verfügbaren Informationen sind natürlich von dieser ausgewählt und damit selektiv. Trotzdem bietet gerade dies manchmal sehr aufschlussreiche Einblicke. Zudem können sich Nutzer sehr einfach über wichtige Geschehnisse im Leben von entfernten Bekannten auf dem Laufenden halten, wenn sich diese entscheiden, Informationen hierzu in ihrem Profil preiszugeben.

b) Anbieterperspektive

Aus Perspektive der Anbieter kommerzieller sozialer Netzwerke stellen die von ihren Nutzern produzierten Daten einen Rohstoff dar, der möglichst gewinnbringend zu nutzen ist.[110] Die Erhebung und Verarbeitung der Daten geschieht entsprechend zu zwei übergeordneten Zwecken: Erstens muss ein Anbieter sozialer Netzwerke stets daran arbeiten, auch in Zukunft eine attraktive Option für alte und neue Nutzer darzustellen, um zu verhindern, dass diese zu

---

109 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 20; Die Autoren stellen aber auch kritisch feststellen, dass eben deshalb die Erstellung einer alternativen „Online-Identität“ in Abgrenzung zu einer „Offline-Identität“ nicht immer möglich und für das Individuum auch nicht immer praktisch sinnvoll ist.

110 *Martini/Fritzsche*, VerwArch 2014, 450 (453 f.).

Konkurrenten abwandern – hieran sind beispielsweise die einst sehr erfolgreichen deutschen VZ-Netzwerke gescheitert.[111] Zweitens muss er die gewonnenen Daten möglichst profitabel verwenden, insbesondere solange es sich um ein formal „kostenloses" Netzwerk handelt, wie es bei Facebook der Fall ist.

aa) Perpetuierung und Vergrößerung des Netzwerkes

Facebook stellt mit seinen 1,6 Milliarden aktiven Nutzern zwar weltweit die unangefochtene Nummer eins auf dem Markt sozialer Netzwerke dar.[112] Einstmals erfolgreiche soziale Netzwerke wie Myspace oder auf dem deutschen Markt die VZ-Netzwerke zeigen aber, dass soziale Netzwerke auch schnell wieder untergehen können, wenn sie an Attraktivität für die Nutzer verlieren. Entsprechend muss es ein Anliegen eines jeden Anbieters sozialer Netzwerke sein, den Bedürfnissen seiner Nutzer nachzugehen und ihnen ein möglichst angenehmes Nutzungserlebnis zu bieten. Zudem ist es gewinnbringend, mehr Nutzer in das Netzwerk zu locken, da dies einerseits durch den größeren Vernetzungseffekt auch die Attraktivität des Netzwerks für alle Nutzer erhöht[113], andererseits aber auch vor allem die Generierung von noch mehr Daten verspricht.[114]

In Bezug auf Facebook kristallisieren sich diese Anforderungen vor allem in einer Förderung der Vernetzung von Nutzern und in der Priorisierung der angezeigten Inhalte innerhalb des Netzwerks. Zudem findet eine ständige Steigerung von dynamischen Inhalten statt, da diese durch die regelmäßige inhaltliche Veränderung eine größere Aufmerksamkeit ihrer Nutzer beanspruchen und sie dazu verleiten, mehr Zeit in dem Netzwerk zu verbringen.[115]

i) Vernetzung von Nutzern

Facebook arbeitet sehr aktiv daran, seine Nutzer besser miteinander zu vernetzen. So gibt es beispielsweise eine Anzeige von „Personen, die du vielleicht kennst". Jedenfalls früher benutzte Facebook zudem den sogenannten „Freunde-Finder", im Rahmen dessen es sich die Erlaubnis

111 Vgl. *Buchner*, Facebook zwischen BDSG und UWG, in: FS Köhler, S. 55, der allerdings zutreffend darauf hinweist, dass die VZ-Netzwerke auch daran scheiterten, sich besonders genau an die Datenschutzgesetze gehalten zu haben und daher transparenter als Konkurrenten wie Facebook den beabsichtigten Datenumgang kommunizierten und hierdurch mediale Aufschreie und Kundenproteste provozierten.

112 Zur Verbreitung sozialer Netzwerke bereits oben unter B.I.2.

113 *Mayer-Schönberger*, Die Tugend des Vergessens, S. 219; *Grimmelmann*, 94 Iowa L.Rev. 1137 (1154 ff.), 2008-2009.

114 Vgl. zur Funktionsweise der Informationsökonomie *Mayer-Schönberger*, Die Tugend des Vergessens, S. 100 ff.

115 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 50.

einholte, auf das Emailadressbuch der zur Registrierung angegebenen Emailadresse zuzugreifen und den Kontakten Beitrittsaufforderungen zu Facebook zu schicken.[116]

Die Vorschläge von Facebook, welche Personen man vielleicht kennt und daher zu den eigenen Kontakten hinzufügen sollte, sind häufig erstaunlich zutreffend. Ermöglicht werden sie Facebook durch statistische Wahrscheinlichkeitsberechnungen und eine Analyse bestehender Kontaktnetzwerke. So ist, in einem einfachen Beispiel, die Wahrscheinlichkeit sehr hoch, dass zwei Nutzer, die auf derselben Schule waren und von dort bereits fast den identischen Kreis an Bekannten in dem sozialen Netzwerk haben, sich auch persönlich kennen. Facebook kann somit Daten, die von Nutzern über die Schule, den Wohnort oder den Arbeitsplatz gemacht werden, dazu nutzen, Vorhersagen zu treffen, welche Leute sich kennen, die diese Bekanntschaft formal noch nicht bestätigt haben.

Ein weit höheres Analysepotential bietet darüber hinaus der durch den „Freunde-Finder" ermöglichten Zugriff auf Emailadressbücher.[117] Auch hier besteht wieder eine hohe Wahrscheinlichkeit, dass sich Personen, die gegenseitig über die Emailadresse des anderen verfügen, kennen. In einem weiteren Schritt ist es für Facebook sogar möglich, mithilfe der Emailadressbücher unterschiedlicher Nutzer verhältnismäßig zuverlässige Vorhersagen darüber zu treffen, ob sich zwei *Nichtmitglieder* kennen.[118] Wenn zum Beispiel der Nutzer A und der Nutzer B jeweils über die Emailadresse des anderen verfügen und zudem auch jeweils die Emailadressen von C und D haben, besteht eine gewisse Wahrscheinlichkeit, dass sich auch C und D gegenseitig kennen. Selbst wenn C und D nicht Mitglieder bei Facebook sind, erfährt Facebook somit etwas über ihr soziales Umfeld.

Facebook kann also über Emailadressbücher erhebliche Rückschlüsse auf „offline" existierende Verbindungen und Netzwerke ziehen.[119] Diese Erkenntnisse können wiederum eingesetzt werden, wenn sich beispielsweise die Nutzer C und D später einmal entscheiden, sich doch ein Profil bei Facebook zuzulegen. In diesem Fall können ihnen sofort die richtigen Vorschläge für Bekanntschaften gemacht werden, damit sie unmittelbar in die soziale Struktur Facebooks eingebunden werden.

---

116 *Von der Lühe*, Perspektive der Nutzer, in: Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co, S. 70; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 16; KG Berlin, ZD 2014, 412 (412 ff.); ausführlich zum „Freunde-Finder", insbesondere zu Fragen der Rechtmäßigkeit, *Maisch*, Informationelle Selbstbestimmung, S. 204 ff.

117 Kritisch zur Rechtmäßigkeit dieser Funktion *Maisch*, Informationelle Selbstbestimmung, S. 207 f. m.w.N.

118 *Horvát*, u.a., One Plus One Makes Three, PLoS ONE 7(4): e34740, S. 5 ff.

119 *Horvát*, u.a., One Plus One Makes Three, PLoS ONE 7(4): e34740, S. 7.

ii) Priorisierung der anzeigten Inhalte

Soziale Netzwerke leben davon, dass die Nutzer sich in ihnen selbst präsentieren und untereinander Informationen austauschen. Diese können sowohl persönlicher Natur, in Form von Statusupdates, Fotos und Ähnlichem, aber auch sachlicher oder unterhaltsamer Natur sein, dann häufig in Form von Links auf andere Webseiten. Diese werden in der Regel nach dem Einloggen auf der Startseite des sozialen Netzwerks präsentiert, bei Facebook im Rahmen der sogenannten „Chronik", früher auch „Timeline", „Newsfeed" oder Pinnwand genannt. Durch die enorme Reichweite und große Nutzerzahlen, insbesondere bei Facebook, ist es aber quasi unmöglich, jeden dieser Posts von „Freunden" einzeln wahrzunehmen. Die Anbieter sozialer Netzwerke haben hierauf reagiert, indem sie Algorithmen entwickelt haben, die auswählen, welche Informationen auf der Titelseite eines Nutzers angezeigt werden.[120]

Die Algorithmen sind so erstellt, dass sie eine für den Nutzer möglichst „interessante" Auswahl treffen. Dies ist zunächst im Interesse des Nutzers, der nicht mit „uninteressanten" Nachrichten behelligt wird. Er erlebt die Nutzung des sozialen Netzwerkes damit als positiver und wird mit größerer Wahrscheinlichkeit länger darin verweilen, seine Nutzung möglicherweise sogar intensivieren. Bereits dies stellt einen Gewinn für den Anbieter des sozialen Netzwerks dar. Darüber hinaus steigert der Anbieter die Wahrscheinlichkeit, dass ein Nutzer eine angebotene Nachricht weiterverfolgt und somit weitere Daten generiert, indem er einen weiteren Einblick in seine Interessen erlaubt.[121] Vergleichbare Algorithmen werden daher auch außerhalb von sozialen Netzwerken angewendet, etwa von Google bei der Präsentation der Suchergebnisse bei einer Recherche: Sämtliche verfügbaren Daten werden genutzt, um einem Nutzer ein möglichst passendes, für ihn „interessantes" Suchergebnis zu bieten und im Folgenden weitere Daten über ihn zu sammeln.[122]

Was zunächst nach einer Win-Win Situation aussieht, birgt in sich das Problem der sogenannten „Filterblase" (im englischen Original: „Filter-Bubble").[123] Indem die angezeigten Inhalte anhand der bisherigen Interessen und Ansichten ausgewählt werden, besteht die Gefahr, Nutzer intellektuell und sozial in einer Blase zu isolieren.[124] Wer beispielsweise auf eine der oben

120 Ausführlich: *Pariser*, Filter Bubble, S. 37 f.
121 *Pariser*, Filter Bubble, S. 37 ff.
122 *Pariser*, Filter Bubble, S. 32 ff.; *Hoffmann-Riem*, Innovation und Recht, S. 622 f.; vgl. auch *Martini*, DVBl. 2014, 1481 (1483).
123 Der Begriff wurde geprägt von *Pariser*, Filter Bubble.
124 *Pariser*, Filter Bubble, S. 125.; *Sandfuchs*, Privatheit wider Willen, S. 26 ff.; vgl. auch *Von der Lühe*, Perspektive der Nutzer, in: Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co, S. 71; *Del Vicario* u.a., PNAS 2016, 554 (556 ff.); *Martini*, DVBl. 2014, 1481 (1484).

beschrieben Arten der Datenpreisgabe zu erkennen gibt, dass er sich eher rechts oder eher links im politischen Spektrum einordnet, wird schnell vorwiegend hierzu passende Informationen angezeigt bekommen.[125] Eine Konfrontation mit widersprüchlichen Positionen, die zu einer kritischen Überprüfung eigener Überzeugungen einladen könnte, wird unwahrscheinlicher, im Extremfall gar verhindert. Stattdessen bilden sich homogene, voneinander abgeschottete Interessengruppen, innerhalb derer sich die Nutzer unwidersprochen und eine absolute Mehrheit repräsentierend wägen.[126] Es wird suggeriert, dass die eigene Meinung die einzig vertretbare ist und die ständige Konfrontation mit ähnlichen Überzeugungen verstärkt diese eigene Meinung durch die Ausbildung eines *confirmation bias* bzw. einer Echokammer.[127]

Mit Blick auf den gesamtgesellschaftlichen, demokratischen Diskurs kann dies ein erhebliches Problem bedeuten. Insbesondere die Kommunikation und der Informationsaustausch verlagern sich zunehmend ins Internet im Allgemeinen und sozialen Netzwerken im Besonderen. Diesen kommt somit zunehmend die Bedeutung eines materiell öffentlichen Raums zu.[128] In einer kürzlich veröffentlichten ausführlichen Studie des *Reuters Institute for the Study of Journalism* gaben durchschnittlich 46% der Nutzer sozialer Medien in der EU an, soziale Medien zum Nachrichtenkonsum zu verwenden – was zwei Dritteln der befragten Facebooknutzer entspricht – und für 10% stellen soziale Netzwerke sogar bereits die Hauptnachrichtenquelle dar.[129]

Eine Gesellschaft, die auf Toleranz und demokratischer Mitbestimmung aufbaut und in der eine gemeinwohlorientierte Abwägung aller Interessen stattfinden muss, ist darauf angewiesen, dass in ihr offen und interessenübergreifend diskutiert wird. Die Filterblase führt indes zu einer Fragmentierung des notwendigen gesamtgesellschaftlichen Diskurses, indem anders lautende Meinungen und Ansichten von der Wahrnehmung ausgeschlossen werden.[130] Natürlich ist festzuhalten, dass auch außerhalb von sozialen Netzwerken im Internet Formen der Filterblasen

---

125 *Pariser*, Filter Bubble, S. 127 f.; vgl. auch *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 37; *Hoffmann-Riem*, AöR 2012, 509 (536 f.).; *Reuters Institute*, http://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital-News-Report-2016.pdf, S. 12 f

126 Vgl. *Pariser*, Filter Bubble, S. 164; *Sandfuchs*, Privatheit wider Willen, S. 28; diese Effekte werden weiter verstärkt, indem Nutzer schwerpunktmäßig solche Informationen aktiv weiterverbreiten, die zu ihrer bisherigen Überzeugung passen, so *Del Vicario* u.a., PNAS 2016, 554 (556 ff.).

127 *Del Vicario* u.a., PNAS 2016, 554 (556 ff.); instruktiv: *Sandfuchs*, Privatheit wider Willen, S. 28 f. m.w.N.

128 *Schliesky u.a.*, Schutzpflichten und Drittwirkung im Internet, S. 120 ff.; *Hoffmann-Riem*, AöR 2012, 509 (512 ff.).

129 *Reuters Institute*, http://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital-News-Report-2016.pdf, S. 8, 10.

130 *Sandfuchs*, Privatheit wider Willen, S. 47 f.; *Pariser*, Filter Bubble, S. 161 ff.; *Del Vicario* u.a., PNAS 2016, 554 (556 ff.); *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 37; *Richter*, Big Data und Demokratische Willensbildung, in: ders. (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 60 ff.; vgl. auch *Hoffmann-Riem*, AöR 2012, 509 (536 f.).; *ders.*, Innovation und Recht, S.628 f.

existieren: Menschen suchen sich bestimmte Interessengebiete und treffen Entscheidungen darüber, mit wem sie längere Kontakte aufbauen. Informationen und Meinungen, die nicht in das eigene Weltbild passen, werden auch außerhalb von sozialen Netzwerken im Internet gerne ausgeblendet.[131] Dennoch ist die Filterblase in sozialen Netzwerken im Internet aus mehreren Gründen hervorhebungswürdig und gegebenenfalls auch regulierungsbedürftig.

Erstens liegen die ihr zugrundeliegenden Algorithmen außerhalb der Kontrolle der Nutzer und arbeiten sehr intransparent.[132] Eine kritische Reflektion darüber, warum gewisse Inhalte präsentiert werden und andere nicht, ist für die Nutzer daher – anders als in der „offline-Welt" – zumindest sehr schwierig. Indem die Existenz der Filterblase nicht transparent gemacht wird, wird es für einzelne Nutzer erschwert, auch andere Meinungen als vertretbar anzuerkennen bzw. überhaupt zu erkennen, inwiefern sie voreingenommen informiert werden.[133] Eine gezielte Änderung der Prioritäten der Filterblase ist für Nutzer zudem nur sehr schwer möglich, da jedenfalls Facebook hierfür keinerlei Funktionen bereithält. Dass Facebook die Zusammenstellung der angezeigten Inhalte völlig transparent macht, ist eher unwahrscheinlich, da dies voraussetzen würde, Nutzern einen sehr detaillierten Einblick darin zu geben, wie viel Facebook tatsächlich über sie weiß und aus den vorhandenen Daten ableiten kann. Es ist jedenfalls nicht unplausibel, dass dies bei vielen Nutzern sogenannte „chilling effects" auslösen würde, die sie zu einer restriktiveren Nutzung sozialer Netzwerke und generell einem vorsichtigeren Umgang mit ihren Daten verleiten würden.[134] Zudem könnten Facebooks Konkurrenten die Methoden sehr einfach kopieren. Beides ist offensichtlich nicht im Interesse Facebooks. Darüber hinaus gesteht zumindest Google auch ein, dass letztendlich nur eine eingeschränkte menschliche Kontrolle und Kenntnis darüber besteht, wie ein Suchergebnis für einen Nutzer der Suchmaschine im Detail erstellt wird. Vielmehr haben komplexe,

---

131 Jedenfalls im Grundsatz stellen dies auch *Del Vicario* u.a., PNAS 2016, 554 (556 ff.) heraus, indem das aktive Verbreitungsverhalten von Nutzern im digitalen Raum sich in homogenen Echokammern gleicher Interessen bewegt.

132 *Pariser*, Filter Bubble, S. 16; *Sandfuchs*, Privatheit wider Willen, S. 29; vgl. auch *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 31 ff.; *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 98 f.; *Reuters Institute*, http://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital-News-Report-2016.pdf, S. 13; vgl. auch *Hoffmann-Riem*, AöR 2012, 509 (537 f.).

133 Vgl. *Pariser*, Filter Bubble, S. 10; *Sandfuchs*, Privatheit wider Willen, S. 29; vgl. auch *Richter*, Big Data und Demokratische Willensbildung, in: ders. (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 61 f.

134 So auch bereits *Hermstrüwer*, Informationelle Selbstgefährdung, S. 367. Ausführlich zu Mechanismen der Selbstzensur aufgrund einer Überwachung: *Sandfuchs*, Privatheit wider Willen, S. 30 ff.; *Mayer-Schönberger*, Die Tugend des Vergessens, S. 131 ff.; vgl. hierzu auch *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 99 f.; *Das/Kramer*, Self-Censorship on Facebook, http://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350, S. 120, 125.

selbstlernende Algorithmen einen erheblichen Einfluss, die sich laufend weiterentwickeln und verbessern, indem sie unter anderem das Feedback verwenden, wie oft angezeigte Inhalte von dem Nutzer weiterverfolgt wurden.[135] Selbst wenn Anbieter sozialer Netzwerke also verpflichtet würden, offenzulegen nach welchen Kriterien die angezeigten Inhalte zusammengestellt werden, ist nicht ganz klar, inwieweit dies überhaupt noch technisch möglich wäre.

Ein zweites Problem ist, dass – zumindest gegenwärtig – die Algorithmen von einer homogenen Identität der Nutzer ausgehen, also im Ergebnis annehmen, dass Nutzer in jeder Situation und gegenüber jedem Menschen dieselben Verhaltensweisen und Ansichten zeigen.[136] Dies ist indes überaus zweifelhaft, da es sicherlich Dinge gibt, die man zwar im Privaten tun oder sagen würde, nicht aber in der Öffentlichkeit oder gegenüber seinem Arbeitgeber.[137] Diese grundlegende Erkenntnis ist im Rahmen der deutschen Grundrechtsdogmatik fest verwurzelt in der Drei-Sphären-Theorie des allgemeinen Persönlichkeitsrechts, welche durch unterschiedliche zu duldende Eingriffe anerkennt, dass sich Menschen je nach Privatheit des Kontextes unterschiedlich verhalten.[138] Im Internet, gerade in sozialen Netzwerken, wird diese Unterscheidung aufgeweicht, indem der Nutzer zu einer einzigen Identität zusammengeführt wird und er basierend auf dieser in statistische Muster einsortiert wird. Daten, die er eigentlich in Nutzung seiner privaten Sphäre erzeugt hat, werden unter Umständen in eine öffentliche Sphäre hineingezogen.[139] Wer beispielsweise, während er in seinen Facebook Account eingeloggt ist, auf mit Social PlugIns versehenen Seiten zur Schuldenberatung surft, riskiert wegen der Reichweitenanalyse, dass dieses Verhalten mit seinem Profil verknüpft wird und er entsprechend Probleme bekommen könnte, gute Kreditkonditionen zu erhalten, sollten diese Daten an eine Bank weitergegeben werden.[140] Gleichzeitig liegt in dieser Annahme der homogenen Identität auch die aktuell noch größte Schwachstelle der Filterblase: Solange der Algorithmus nicht zahlreiche weitere Datensätze in den Rechnung mit einbezieht, kann er nicht ermitteln, ob eine Person aus Überzeugung auf einen Link klickt oder aus Interesse am Widerspruch.[141] Gerade bei politisch sehr interessierten Nutzern, die sich auch gerne mit von

---

135 *Pariser*, Filter Bubble, S. 13; vgl. auch *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 33.

136 *Pariser*, Filter Bubble, S. 109 ff.

137 *Pariser*, Filter Bubble, S. 116 f.

138 Instruktiv: *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 149 ff.

139 Deshalb kritisch zur Anwendbarkeit der Drei-Stufen-Theorie auf Fragen der informationellen Selbstbestimmung im Internet: *Simitis*, in: Simitis, BDSG, § 1 Rn. 65 ff.; *Nebel*, ZD 2015, 517 (518 f.); *Geminn/Roßnagel*, JZ 2015, 703 (706). Hierzu noch vertieft unten unter D.I.3.b)aa)ii).

140 *Pariser*, Filter Bubble, S. 118 f.; hierzu auch noch ausführlich sogleich unten unter B.II.3.b)bb)iii).

141 *Pariser*, Filter Bubble, S. 117 f.

ihnen abweichenden Meinungen befassen, kann dies dazu führen, dass sie zunächst sehr viel mehr Inhalte von dieser abweichenden Meinung angezeigt bekommen als sie eigentlich wollen. Konkret bedeutet dies, dass sie mehr Statusupdates von Kontakten erhalten, die diese Meinung teilen und auch verstärkt Werbung zu Produkten erhalten, die andere Nutzer mit dieser politischen Einstellung interessiert. Da dies Facebooks Interesse zuwiderläuft, seinen Nutzern Angebote zu machen, die sie aufrichtig interessieren, ist davon auszugehen, dass die Algorithmen in Zukunft dahingehend verfeinert werden, auch noch die vermeintliche Absicht eines Nutzers erkennen zu können, wenn er auf Links und andere Angebote klickt, um dies in die Erstellung der vermeintlichen Identität einfließen zu lassen.

Ein drittes Problem kann in der möglichen Radikalisierung des Diskurses liegen. Indem in sozialen Netzwerken jedenfalls faktisch pseudonym und mit wenig Aufwand eine Empörungskultur betrieben werden kann, etablieren sich teilweise sehr raue Umgangsformen. Radikale Mindermeinungen können direkt an Medienkonsumenten herangetragen werden und genießen eine relative Öffentlichkeit. Da das Hinterlassen eines Posts in sozialen Netzwerken regelmäßig mit wenig direkten Konsequenzen verknüpft ist, sammeln sich schnell zustimmende Kommentare, die aufgrund der oben beschriebenen Mechanismen der Homogenisierung eine einheitliche Empörungsfraktion suggerieren. Hierdurch entsteht ein erhebliches verbales Eskalationspotential für derartige Diskussionen.[142]

Im Ergebnis stellt die Filterblase damit nicht nur ein potentielles gesellschaftliches Problem aufgrund der Fragmentierung und möglichen Radikalisierung des Diskurses dar; vielmehr kann sie auch auf individueller Ebene eine erhebliche Einschränkung der individuellen Persönlichkeitsentfaltung bedeuten. Der informatorische Horizont eines Nutzers kann deutlich beschränkt werden. Auch seine persönliche Entwicklung und Ausbildung von neuen Interessen können erschwert werden, indem die Konfrontation mit Neuem nur noch danach ausgewählt wird, wie er sich in der Vergangenheit entschieden hat.[143] Anders als in der „offline-Welt“ hat der Nutzer nur sehr wenig Kontrolle über die Impulse, die an ihn herangetragen werden, da diese von einem intransparenten Algorithmus gesteuert werden. Eine vollständige Abschottung von anderen Ansichten ist in der Gesellschaft zwar möglich, aber schwierig. Innerhalb von sozialen Netzwerken ist dies bedeutend einfacher, indem im wahrsten Sinne des Wortes eine virtuelle Realität für den Nutzer konstruiert wird.

---

142 Ausführlich hierzu aus psychologischer und sozialwissenschaftlicher Sicht: *Schaarschmidt*, Die Brandstifter aus dem Netz, in: Gehirn und Geist, Spektrum der Wissenschaft, 5/2016, S. 32 f.

143 *Martini*, DVBl. 2014, 1481 (1484) spricht insoweit auch von versteinerten Profilen und dem Internet als gleichsame „Asservatenkammer für Daten“.

bb) Generierung „profitabler" Daten

Die Auswertung aller verfügbaren Daten zur Generierung von profitablen Persönlichkeitsprofilen ist der Kern von Facebooks Geschäftsmodell.[144] Im Folgenden soll skizziert werden, auf welche Arten Facebook die oben genannten Datenarten verwenden kann, um aus ihnen Persönlichkeitsprofile seiner Nutzer zu erstellen und seinen enormen Jahresumsatz von 12,47 Milliarden US-Dollar im Jahr 2014[145] und sogar 17,93 Milliarden US-Dollar im Jahr 2015[146] zu erwirtschaften.

i) Erstellung von Persönlichkeitsprofilen

Auch wenn die Auswertung der Nutzerdaten zu Persönlichkeitsprofilen im Detail Geschäftsgeheimnissen Facebooks unterliegt, lassen sich auf allgemeiner, abstrakter Ebene dennoch einige Feststellungen hierzu treffen.[147] Wichtig ist hierbei, dass Facebook zur Erstellung der Persönlichkeitsprofile nicht nur auf die Angaben zurückgreift, die von den Nutzern unmittelbar in ihrem Profil gemacht wurden. Vielmehr werden die umfangreichen Daten der Reichweitenanalyse mit einbezogen und zusätzliche statistische Auswertungen angestellt.

Es wurde oben bereits angedeutet, dass die bewusst von Nutzern zur Verfügung gestellten Profil- und Statusdaten über sich selbst nur einen sehr kleinen Teil der für Facebook verfügbaren Daten ausmachen. Ein sehr viel größerer Teil entfällt auf die im Rahmen der Nutzung anfallenden Verkehrs- und Nutzungsdaten, sowie insbesondere die über Social PlugIns erhobenen Reichweitendaten.[148]

Bereits durch das Speichern der besuchten Webseiten lassen sich erhebliche Rückschlüsse auf die Interessen des Nutzers, sowie seine allgemeine Lebenssituation ziehen. Beispiele hierfür sind die bereits genannten Aufrufe von Vergleichsportalen für Flugreisen, Nachrichtenseiten, Onlineshops, Jobbörsen, Partnerbörsen oder Seiten zur Schuldnerberatung. Bereits für diese Informationen besteht ein Schutzbedürfnis, da sie in den Händen der falschen Person – etwa

144 *Spiecker gen. Döhmann*, K&R 2012, 717 (718); *Greve*, Drittwirkung, in: FS Kloepfer, S. 668.

145 Facebook Inc., Form 10-k für die amerikanische SEC, abgegeben am 29.01.2015 für den Zeitraum bis 31.12.2014, S. 62; Facebook Annual Report 2014, S. 43.

146 Facebook Annual Report 2015, S. 43.

147 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 55 ff.; vgl. beispielsweise auch für die Geheimhaltung der Scoreformel der SCHUFA: BT-Drs. 16/10529, S. 17, sowie *Martini*, DVBl. 2014, 1481 (1485) m.w.N.; vgl. auch bereits *Maisch*, Informationelle Selbstbestimmung, S. 168 ff.

148 *Von der Lühe*, Perspektive der Nutzer, in: Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co, S. 71; *Spindler*, GRUR-Beilage 2014, 101 (105); *Ernst*, NJOZ 2010, 1917 (1917).

des Arbeitsgebers, Ehepartners oder auch der Krankenversicherung – offensichtliche negative Konsequenzen auslösen können.[149]

Weitere Informationen lassen sich durch eine Analyse des Kontakte- bzw. Freundeskreises innerhalb des sozialen Netzwerks generieren. Aus der Häufigkeit und Form von Kommunikation mit den Kontakten können Rückschlüsse auf die soziale Stellung einer Person innerhalb des persönlichen Netzwerks gezogen werden, welche wiederum Rückschlüsse auf allgemeine charakterliche Merkmale zulässt.[150] Darüber hinaus lassen sich aus vielen gemeinsamen Interessen oder Hintergründen Informationen über einen Nutzer ableiten. Wenn beispielsweise 90% der Kontakte eines Nutzers auf eine bestimmte Schule oder Universität gehen, liegt der Schluss nahe, dass auch dieser Nutzer dort angemeldet ist, selbst wenn er sich entschieden hat, diese Information nicht in seinem Profil zu teilen. Ebenso kann eine Analyse der Facebook-Kontakte mit einer hohen Treffsicherheit die sexuelle Orientierung eines Nutzers aufdecken.[151] Das Profil eines Nutzers ist daher niemals isoliert zu betrachten, sondern stets „vor dem Hintergrund seiner sozialen Kontakte“ und im Kontext aller sonstigen verfügbaren Daten.[152]

Das wahre Potential der gesammelten Daten liegt aber im Abgleich mit statistischen Mustern, die aus großen Datensammlungen im Rahmen von Big Data Analysen gewonnen werden.[153] So

---

149 *Riefa/Markou*, Online Marketing, in: Savin/Trzaskowski (Hrsg.) Research Handbook on EU Internet Law, S. 399 f.

150 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 50; *Karg/Fahl*, K&R 2011, 453 (455); *Kosinski/Stillwell/Graepel*, PNAS 2013, 5802 (5802 f.); *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 97; *Greve*, Drittwirkung, in: FS Kloepfer, S. 669.

151 *Horvát*, u.a., One Plus One Makes Three, PLoS ONE 7(4): e34740, S. 1 m.w.N.; *Kosinski/Stillwell/Graepel*, PNAS 2013, 5802 (5803); *Sandfuchs*, Privatheit wider Willen, S. 22; *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 28 f.; *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 97 f.; *Martini/Fritzsche*, VerwArch 2014, 450 (454); vgl. auch Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 8.

152 *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 20; vgl. auch *Hill*, DÖV 2014, 213 (218); *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 97 f.

153 Instruktiv: *Sandfuchs*, Privatheit wider Willen, S. 16 f.; *Riefa/Markou*, Online Marketing, in: Savin/Trzaskowski (Hrsg.) Research Handbook on EU Internet Law, S. 397 ff.; *Martini*, DVBl. 2014, 1481 (1482 f.); *Hill*, DÖV 2014, 213 (216 f.); *Ders./Fritzsche*, VerwArch (104) 2013, 449 (454); *Weichert*, ZD 2013, 251 (253 f.); *Spiecker gen. Döhmann*, K&R 2012, 717 (720 f.); *Strahilevitz*, 126 Harv. L. Rev. 2010 (2021 ff.) 2012-2013; BT-Drs. 18/4631, S. 22; vgl. auch *Kühling/Sivridis/Schwuchow/Burghardt*, DuD 2009, 335 (340); Ein aktuelles Problem der Regulierung von Big Data Analysen ist, dass sie der bisherigen Datenschutzgesetzgebung nicht unterfallen, solange sie statistische Auswertungen anonymer – und damit nicht personenbezogener – Daten betreffen. Erst in der Anwendung der erstellten Muster auf einzelne Personen greift wieder das Datenschutzrecht, vgl. *v. Lewinsky*, Matrix des Datenschutzes, S. 56, 59, der insoweit von einem „blinden Fleck des Datenschutzrechts“ spricht. Gleichzeitig besteht durch immer größere Datensätze, die miteinander verknüpft werden, aber auch ein höheres Risiko einer Re-Identifizierbarkeit von eigentlich anonymisierten Daten, vgl. *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 28 m.w.N.

stellen beispielsweise die Daten, wo ein Nutzer wohnt, zu welcher Schule er gegangen ist, wie lange er sich im Internet aufhält und welche Musikrichtung er bevorzugt, für sich genommen noch keine allzu sensiblen Angaben dar. Ganz anders sieht dies aus, wenn sich im Rahmen einer Analyse zahlreicher Nutzer ergibt, dass solche mit einer vergleichbaren Kombination eine statistisch signifikant erhöhte Wahrscheinlichkeit aufweisen, chronisch krank, straffällig, arbeitslos, überschuldet oder anderweitig auffällig zu werden.[154] In Ansätzen ist diese Form der Analyse von der Schufa bekannt, die seit jeher unter anderem die aktuelle und die bisherigen Adressen von Kreditnehmern aufnimmt und damit die Möglichkeit erhält, diese zur Berechnung des individuelles Kreditscores beispielsweise in Relation zu dem Einkommens- und Kriminalitätsspiegel in der Umgebung zu setzen.[155] Angesichts der sehr viel größeren Datenmengen, die insbesondere Facebook zur Verfügung steht, lässt sich erahnen, wie viel genauer und präziser solche Analysen ausfallen können.

Untersuchungen weisen insoweit sehr konkret nach, dass sich bereits allein anhand der „Likes" eines Nutzers, also Interessenbekundungen für bestimmte Meinungen, politische Seiten, Produkte, Musikrichtungen oder Ähnliches, detaillierte Aussagen über die Person des Nutzers getroffen werden können.[156] So ist es beispielsweise amerikanischen Forschern gelungen, anonyme US-amerikanische Profile ohne Fotos mit sehr hoher Treffsicherheit dem Geschlecht, der Hautfarbe, der politischen Grundeinstellung, der Religiosität und Ähnlichem zuzuordnen, ohne dass diese direkt in das Profil eingetragen worden wären.[157]

Obgleich somit Wert darauf gelegt wird, den individuellen Nutzer so präzise wie möglich zu charakterisieren und zu durchleuchten, dient diese Charakterisierung letztlich nur der präzisen Zuordnung zu einer größeren statistischen Gruppe. Erst im Zusammenhang mit dem Verhalten dieser Gruppe können nämlich Prognosen über das zukünftige individuelle Verhalten getroffen werden.[158] Ironischerweise findet somit im Zuge der zunehmend detaillierteren Analyse von Individuen eine Entindividualisierung auf der Entscheidungsebene statt, indem es dort weniger

---

154 Vgl. *Martini*, DVBl. 2014, 1481 (1482 f.).

155 Während eine Auskunftspflicht der Schufa gegenüber einem Betroffenen besteht, welche Faktoren in die Berechnung des Scorewertes einfließen, unterliegt die genaue Formel zur Berechnung des Scorewertes dem Geschäftsgeheimnis der Schufa, so BGH, ZD 2014, 306 (307 f.) Rn. 22 ff.; vgl. auch *Buchner*, Informationelle Selbstbestimmung, S. 121 ff.; vgl. allgemein zum Potential der Datenauswertung bereits vor Big Data *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 28 f.

156 *Kosinski/Stillwell/Graepel*, PNAS 2013, 5802 ff.

157 *Kosinski/Stillwell/Graepel*, PNAS 2013, 5802 ff.

158 *Sandfuchs*, Privatheit wider Willen, S. 16 f.; *Martini*, DVBl. 2014, 1481 (1482 f.); *Peifer*, K&R 2011, 543 (543); vgl. auch *Hill*, DÖV 2014, 213 (218) m.w.N.; *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 26; diese Dimension der statistischen Analyse verkennt *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 46 f., 59 f.

auf die konkreten Umstände des Einzelfalls ankommt als auf die Parallelen zu zuvor identifizierten statistischen Mustern.[159] Das Individuum wird somit zu einem bloßen Träger von Gruppenmerkmalen und hieraus prognostiziertem zukünftigen Verhalten degradiert, mit einer erhöhten Diskriminierungsgefahr aufgrund einzelner Merkmale.[160] Zudem besteht das Risiko, dass Entscheidungen immer weniger aufgrund von wissenschaftlich nachprüfbarer Kausalität und mehr aufgrund von statistisch ermittelter Korrelation getroffen werden. Da eine Korrelation mögliche Zusammenhänge aber nur beschreibt und keine Antworten auf die zugrundeliegenden Ursachen gibt, kann hierdurch die Tiefe und Begründetheit der Abwägung erheblichen Schaden nehmen.[161]

Neben dem abstrakten – legitimen – Interesse an informationeller Selbstbestimmung stellen eben diese Veränderungen der Entscheidungsfindung auch einen der zentralen Gründe für die Notwendigkeit einer datenschutzrechtlichen Regulierung der Profilerstellung dar. Es sollte klar geworden sein, dass ein erheblicher Teil der Daten und Informationen, die für die Profilerstellung verwendet werden, nicht bewusst von dem Nutzer preisgegeben werden.[162] Ihnen fehlt entsprechend auch die Kontrolle darüber, welches Wissen insbesondere durch Facebook über sie generiert und an Dritte weitergegeben wird. In dem Maße, in dem relevante Entscheidungen etwa über eine Jobvergabe, eine Kreditvergabe oder eine Krankenversicherung von der im Rahmen der Persönlichkeitsprofilerstellung getroffenen Annahmen abhängen können, wandelt sich das abstrakte Selbstbestimmungsinteresse des Nutzers zu einer sehr konkreten Frage der möglichen Freiheitsausübung.[163] Entsprechend wichtig ist es, den Nutzern effektive Rechte zur Verfügung zu stellen und geltende Rechte konsequent durchzusetzen, um Kontrolle über die Datenpreisgabe und -verwendung zu erlangen.[164]

---

159 *Martini*, DVBl. 2014, 1481 (1485, 1488); vgl. auch *Sandfuchs*, Privatheit wider Willen, S. 17.

160 *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 36 f.

161 Ausführlich *Hill*, DÖV 2014, 213 (216 ff.); vgl. auch *Boehme-Neßler*, DVBl. 2015, 1282 (1283).

162 Ausdrücklich auch *Riefa/Markou*, Online Marketing, in: Savin/Trzaskowski (Hrsg.) Research Handbook on EU Internet Law, S. 398 f.; vgl. auch *Sandfuchs*, Privatheit wider Willen, S. 14 ff.

163 *Greve*, Drittwirkung, in: FS Kloepfer, S. 668 f.; vgl. auch *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 54 f.; die Bundesregierung schreibt hierzu in ihrer Begründung für einen Gesetzentwurf zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts vom 15. April 2015 an, BT-Drs. 18/4631, S. 22: „Die durch die Bildung von Persönlichkeits- und Nutzungsprofilen gewonnenen Informationen können erhebliche Auswirkungen für Verbraucher haben, wenn sie dazu genutzt werden, das Verhalten oder die Marktchancen von Verbrauchern zu beeinflussen (z. B. Scoring)."

164 *Weichert*, ZD 2013, 251 (256 ff.); ebenfalls zustimmend und darüber hinausgehend ein „Algorithmenkontrollrecht" fordernd: *Martini*, DVBl. 2014, 1481 (1481, 1488 f.). Ausführlich zu Fragen der Rechtssetzung und Rechtsdurchsetzung im Bereich der Internetkommunikation: *Hoffmann-Riem*, Innovation und Recht, S. 643 ff.

ii) Personalisierte Werbung

Von den 12,47 Milliarden US-Dollar Gesamtumsatz, die Facebook 2014 erwirtschaftete, entfielen 11,49 Milliarden US-Dollar auf Werbeeinnahmen.[165] Diese Zahlen weisen bereits unmissverständlich darauf hin, dass Facebook in allererster Linie ein Geschäft mit Werbung macht.[166] Angesichts der Vielzahl von Produkten und Anbietern, aber auch der quasi unbegrenzten Werbefläche auf Internetseiten, wird es für den einzelnen Anbieter immer schwieriger, mit seiner Werbung zielgerichtet potentielle Kunden zu erreichen. Die Effektivität allgemeiner Werbung nimmt hierdurch rapide ab, da sie aufgrund einer Reizüberflutung zunehmend ausgeblendet wird. Das Versprechen der Anbieter sozialer Netzwerke ist, so detaillierte Persönlichkeitsprofile erstellen zu können, dass Unternehmen ihre Werbung zielgerichtet und wiederholt jenen anzeigen lassen, die an dem beworbenen Produkt auch grundsätzlich Interesse haben.[167] Darüber hinaus gibt es Anhaltspunkte dafür, dass eine stark personalisierte Werbung rationale Entscheidungsprozesse der Konsumenten umgehen kann, indem sie auf die persönlichen Vorlieben abstellt und auf impulsives Verhalten setzt.[168] Weiß der Werbeträger, was die geheimen Wünsche und Werte seines potentiellen Kunden sind, kann er sich dieser individuell bedienen und somit sehr viel gezielter suggerieren als mit flächendeckender, herkömmlicher „Standard-Werbung". Da die dahinter stehende Personalisierung und Datenanalyse dem Kunden verborgen bleibt, führt sie im Ergebnis zu einem Wissensvorsprung des Werbetreibenden gegenüber dem Konsumenten über dessen eigene Vorlieben und Entscheidungsprozesse. Ein solches Informationsgefälle könnte geeignet sein, die rationale Entscheidungsfindung des Konsumenten signifikant einzuschränken.

Im Markt der Internetwerbung sind Persönlichkeitsprofile von zentraler Bedeutung. Webseitenbetreiber stellen auf ihren Webseiten bestimmte Flächen für Werbezwecke zur Verfügung und erhalten Geld, wenn ein Nutzer auf die angezeigte Werbung geklickt hat oder zumindest die Seite aufgerufen und die Werbung angezeigt bekommen hat.[169]

---

165 Facebook Inc., Form 10-k für die amerikanische SEC, abgegeben am 29.01.2015 für den Zeitraum bis 31.12.2014, S. 62; Facebook Annual Report 2014, S. 43.

166 Vgl. auch *Piltz*, Soziale Netzwerke, S. 23 f.; *Chmelik*, Social Network Sites, S. 79 ff.; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 351; *Dieterich*, ZD 2015, 199 (199); *Peifer*, K&R 2011, 543 (545); ausführlich auch: Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 5 ff.

167 *Riefa/Markou*, Online Marketing, in: Savin/Trzaskowski (Hrsg.) Research Handbook on EU Internet Law, S. 398; *Arning/Moos*, ZD 2014, 126 (126 f.); *Lichtnecker*, GRUR 2013, 135 (135 f.); vgl. auch *Sandfuchs*, Privatheit wider Willen, S. 16.

168 *Pariser*, Filter Bubble, S. 120 ff.

169 *Arning/Moos*, ZD 2014, 242 (242 f.); vgl. auch *Maisch*, Informationelle Selbstbestimmung, S. 166 f.

Im Rahmen des klassischen Online Behavioral Advertising können werbetreibende Unternehmen pauschal im Voraus bestimmte Werbeflächen auf Webseiten buchen. Sobald (irgend-)ein Nutzer die Webseite besucht, wird geprüft, ob er nach dem über ihn verfügbaren Nutzerprofile mit der vorab definierten Zielgruppe übereinstimmt und er erhält gegebenenfalls die standardisierte, zuvor gebuchte Werbung angezeigt.[170] Unterschiedliche Nutzer können somit beim Aufruf derselben Webseite verschiedene Werbung angezeigt bekommen.

Eine noch genauere Abstimmung auf die Interessen des jeweiligen Nutzers erlaubt das sogenannte „Real-Time-Advertising". Dessen Prozess lässt sich vereinfacht wie folgt beschreiben: Der Webseitenbetreiber vermietet gleichsam seine Werbeflächen an ein auf die Vermittlung von Werbung spezialisiertes Unternehmen. Dieses Unternehmen verfügt über zahlreiche Werbeaufträge von anderen werbetreibenden Unternehmen, die ihre Werbung an den potentiellen Kunden bringen wollen. Sobald ein Nutzer eine Webseite aufruft, auf der Werbeflächen vorhanden sind, findet im Hintergrund, unbemerkt vom Nutzer, innerhalb von Mikrosekunden eine automatische Versteigerung der Werbefläche unter den werbetreibenden Unternehmen statt.[171] Diese Versteigerung wird von dem auf die Werbung spezialisierten Unternehmen durchgeführt. Es berechnet anhand von Persönlichkeitsprofilen, die ihm über diesen individuellen Nutzer bekannt sind, wie interessiert dieser Nutzer an den jeweils zur Wahl stehenden Werbeprodukten wäre. Das Ergebnis wird Algorithmen der werbenden Unternehmen mitgeteilt, die daraufhin auf die Anzeige ihrer Werbung bieten können. Das Unternehmen, welches das höchste Angebot für diesen Nutzer macht, erhält den Zuschlag, so dass seine Werbung auf der Webseite angezeigt wird.[172] Anders als beim klassischen Online Behavioral Advertising fallen die Kosten für das Einblenden der Werbung für das werbetreibende Unternehmen erst im Zeitpunkt des Zuschlags an.[173]

In diesem Geschäftsmodell liegt es auf der Hand, dass immer detailliertere Persönlichkeitsprofile und eine genaue Zuordnungsbarkeit zu dem konkreten Nutzer einen erheblichen Vorteil darstellen, da das Risiko von Fehlinvestitionen in Form uninteressanter Werbeanzeigen für alle Beteiligten minimiert wird.[174] Indem sich Facebook auf die Erstellung

---

170 *Arning/Moos*, ZD 2014, 242 (242); vgl. auch *ders./ders.*, ZD 2014, 126 (127).

171 Eine ausführliche Darstellung dieses Prozesses und der beteiligten Akteure, sowie eine Analyse der Rechtmäßigkeit bieten *Arning/Moos*, ZD 2014, 242 ff.

172 *Arning/Moos*, ZD 2014, 242 (243).

173 *Arning/Moos*, ZD 2014, 242 (242 f.).

174 *Arning/Moos*, ZD 2014, 242 (242); vgl. auch *ders./ders.*, ZD 2014, 126 (126); *Maisch*, Informationelle Selbstbestimmung, S. 161 f.

und laufende Verfeinerung eben dieser Persönlichkeitsprofile spezialisiert, schafft es sich eine zuverlässige Einnahmequelle angesichts zahlreicher interessierter Abnehmer für die Profile.

Darüber hinaus generiert Facebook Werbeeinnahmen, indem es direkt innerhalb des sozialen Netzwerks personalisierte Werbung schaltet. Zwar werden nicht direkt klassische Werbeanzeigen eingeblendet. Es gibt allerdings für Unternehmen die Möglichkeit, „gesponsorte Beiträge" zu verfassen, die gegen die Zahlung eines bestimmten Betrags an Facebook besonders weit oben in der Timeline von interessierten Nutzern platziert werden. Gelegentlich sind diese Beiträge auf den ersten Blick gar nicht als Werbung zu erkennen, sondern wirken wie ein normaler Beitrag von anderen Kontakten des Nutzers.[175] Es ist jedenfalls nicht abwegig, anzunehmen, dass es sich daher um eine effektivere Form der Werbung als eine bloße Anzeige auf einer Webseite handelt und dass Facebook sich diese Effektivitätssteigerung entsprechend vergüten lässt. Dies gilt umso mehr, als Facebook mit seinen 1,6 Milliarden Nutzern eine sehr große potentielle Reichweite für eine gebuchte Werbung garantieren kann.

iii) Risikoprognosen

Die im Rahmen der Persönlichkeitsprofilerstellung ableitbaren Risikoprognosen können für zahlreiche wirtschaftliche Akteure – ebenso wie den Staat, der hier aber außer Betracht bleiben soll – von großem Interesse sein. Insbesondere Banken und Versicherungsunternehmen haben ein Interesse daran, ihre potentiellen Kunden vorab gut einschätzen zu können. Dagegen ist grundsätzlich auch nichts einzuwenden, da derartige Informationen essentiell sind, um eine privatautonome, informierte Entscheidung über einen Vertragsschluss treffen zu können.[176] Ein Problem ergibt sich dann, wenn ein Informationsgefälle geschaffen wird, in welchem eine Person nicht mehr wissen kann, welche Informationen über ihn bei dem Vertragspartner vorhanden sind. Seine Chancen auf eine Teilnahme am Wirtschaftsgeschehen können signifikant begrenzt werden, wenn er beispielsweise aufgrund von Big Data Analysen in eine für ihn ungünstige Vergleichsgruppe sortiert wurde.[177] Darüber hinaus ergäbe sich ein strukturelles Machtgefälle von großen Wirtschaftsunternehmen gegenüber Individuen, wenn erstere unkontrolliert über Persönlichkeitsprofile verfügen könnten. Letztendlich ist dies die

---

175 Vgl. *Lichtnecker*, GRUR 2013, 135 (138 f.), der zurecht auf hieraus resultierende Probleme der Schleichwerbung verweist.

176 Ausführlich: *Buchner*, Informationelle Selbstbestimmung, S. 87 f., 118 ff.

177 *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 26 ff.; *Martini*, DVBl. 2014, 1481 (1488); vgl. auch *Weichert*, ZD 2013, 251 (257 f.); BT-Drs. 18/4631, S. 22.

privatwirtschaftliche Fortsetzung der Feststellungen des Bundesverfassungsgerichts im Volkszählungsurteil zur Bedeutung der informationellen Selbstbestimmung gegenüber dem Staat.[178]

Allerdings ist nicht abschließend bekannt, ob und gegebenfalls in welchem Umfang Facebook die erstellten Persönlichkeitsprofile auch tatsächlich an entsprechende Wirtschaftsakteure verkauft und weitergibt. Facebooks eigene Angaben in der Datenrichtlinie, an wen Daten weitergegeben werden, bleiben insoweit denkbar vage.[179] Dennoch scheint es jedenfalls so zu sein, dass sich die Datenweitergabe aktuell auf weitgehend anonymisierte Persönlichkeitsprofile zu Werbezwecken beschränkt. Dies ist sicherlich eine erfreuliche Nachricht für die informationelle Selbstbestimmung der Nutzer. Es ändert aber wenig an der Tatsache, dass die erhobenen Daten und erstellten Persönlichkeitsprofile jedenfalls zu entsprechenden Risikoprognosen verwendet werden könnten und entsprechend eine Notwendigkeit für datenschutzrechtliche Regelungen in diesem Bereich existiert.

iv) Individual Pricing

Unternehmen wie Google und Amazon forschen an Möglichkeiten, für jeden Kunden im Internet einen individuellen Preis zu berechnen, nämlich den maximalen Preis, den dieser Kunde für ein bestimmtes Produkt bereit wäre zu bezahlen (sogenanntes „Individual Pricing“). Auch diese Berechnungen werden durch Persönlichkeitsprofile der Nutzer ermöglicht.[180] Angesichts der Bestrebungen Facebooks, seinen Nutzern direkt Produkte anzubieten und über das soziale Netzwerke bezahlen zu lassen[181], ist es allenfalls eine Frage der Zeit, bis sich die Frage des Individual Pricing auch unmittelbar in diesem Zusammenhang stellt.

Der primäre Nutzen des Individual Pricing liegt für Unternehmen offenkundig darin, dass die Konsumentenrente vollständig zugunsten der Produzentenrente abgeschöpft wird. Anstatt ein Produkt zu einem Gleichgewichtspreis auf dem Markt anzubieten, könnten Unternehmen, die über die individuelle Zahlungsbereitschaft und Wertschätzung eines Kunden informiert sind, ihre Preise entsprechend anpassen und ihren Gewinn damit maximieren. Zudem können neue

178 BVerfGE 65, 1 (40 ff.).

179 „Wir arbeiten mit Drittunternehmen zusammen, die uns dabei helfen, unsere Dienste bereitzustellen und zu verbessern; sie setzen auch Werbeanzeigen oder ähnliche Produkte ein, die es uns ermöglichen, unsere Unternehmen zu betreiben und den Menschen weltweit kostenlose Dienste anzubieten.“ https://www.facebook.com/privacy/explanation (Stand 29. September 2016).

180 *Sandfuchs*, Privatheit wider Willen, S. 17 m.w.N.; *Newman*, 40 William Mitchell L. Rev., 849 (865 ff.), 2013-2014.

181 Hierzu bereits oben unter B.II.2.b)cc).

Kunden angeworben werden, indem mit speziell zugeschnittenen Sonderangeboten ein idealer Neueinstiegspreis angeboten wird. In Kombination mit dem verhaltensökonomisch zu beobachtenden Status Quo Bias vieler Konsumenten, der diese dazu verleitet, bei einem einmal gewählten Produkt zu bleiben,[182] kann dies mittelfristig zu erheblichen Umsatzsteigerungen führen.[183]

An dieser Stelle kann keine umfangreiche Analyse der Wirtschaftlichkeit, Rechtmäßigkeit oder sozialethischen Angemessenheit des Individual Pricing erfolgen. Stattdessen sei nur schlagwortartig auf einige individuelle und gesamtgesellschaftliche Probleme hingewiesen.

Auf individueller Ebene stellt Individual Pricing eine erhebliche Benachteiligung des Kunden dar, da durch die vollständige Abschöpfung der Konsumentenrente einseitig Geld zugunsten der Unternehmen umverteilt wird. Diese Umverteilung wirkt umso stärker, je präzisere Informationen über den einzelnen Kunden verfügbar sind. Das bedeutet, Personen, die in der Lage sind, eine detaillierte Erstellung von Persönlichkeitsprofilen über sich durch entsprechende Datenschutzmaßnahmen zu unterbinden, haben einen Vorteil. Diese Unterbindung setzt aktuell einige Kenntnisse und Engagement voraus. Individual Pricing würde sich daher vor allem auf weniger Engagierte und weniger gebildete Personen auswirken, die keine Zeit oder Mühe dafür erübrigen können oder wollen, sich einer solchen Profilbildung zu entziehen.[184] Gerade solche Personen sind aber tendenziell schon heute eher sozial benachteiligt. Individual Pricing birgt damit – wenn es nicht reguliert wird – das Potential, sozial schwächere Personen unverhältnismäßig stark zu belasten und eine Zweiklassengesellschaft bei der Preisbildung im Internet zu erzeugen.[185]

Für die Personen, die sich entscheiden, die Profilbildung zu unterbinden oder jedenfalls zu stören, können sich Freiheitseinschränkungen ergeben, indem sie gezwungen sind, sich im Internet anders zu verhalten als sie dies normalerweise tun würden.[186] So können sie sich etwa gezwungen sehen, eigentlich nützliche und notwendige Cookies abzulehnen, weil sie Sorge

---

182 Instruktiv: *Thaler/Sunstein*, Nudge, S. 55 ff.

183 Ausführlich: *Newman*, 40 William Mitchell L. Rev., 849 (867 ff.), 2013-2014; vgl. auch *Hermstrüwer*, Informationelle Selbstgefährdung, S. 156 f.

184 *Newman*, 40 William Mitchell L. Rev., 849 (868 f.), 2013-2014; *Strahilevitz*, 126 Harv. L. Rev. 2010 (2029 ff.) 2012-2013; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 154 ff.; vgl. insoweit allgemein zum Selbstschutz im Kontext der Informationsgesellschaft bereits *Hoffmann-Riem*, AöR 1998, 513 (536 f.).

185 *Newman*, 40 William Mitchell L. Rev., 849 (865 ff.), 2013-2014; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 156 f.

186 *Riefa/Markou*, Online Marketing, in: Savin/Trzaskowski (Hrsg.) Research Handbook on EU Internet Law, S. 400.

haben, dass diese auch Informationen über ihr Verhalten sammeln.[187] Darüber hinaus könnten sie auf den Aufruf mancher Webseiten gänzlich verzichten, um bestimmte Interesse nicht preiszugeben oder umgekehrt zahlreiche uninteressante Webseiten aufrufen, um ihre eigentlichen Interessen zu verschleiern. Zwar gibt es Programme, die derartige Aufrufe im Hintergrund automatisch erledigen; hierbei dürfte es sich aber zum einen um ein klassisches Wettrüsten handeln, indem auch Möglichkeiten entwickelt werden, einen solchen automatischen Aufruf von einem echten Nutzeraufruf zu unterscheiden. Zum anderen ist es nicht ohne Risiko, da dem Nutzer so erst Recht der Einfluss darauf verloren geht, welche Daten in die Erstellung seines Persönlichkeitsprofils mit einfließen.

Es fällt auch nicht schwer, sich Konstellationen zu überlegen, in denen Individual Pricing missbraucht werden könnte, indem Produkte, auf die ein Kunde ersichtlich angewiesen ist, nur teurer verfügbar gemacht werden.[188] Verhältnismäßig harmlose Beispiele sind das Angebot einer verteuerten Rückfahrkarte nach dem Kauf einer Hinfahrkarte, oder die Onlinebuchung von Hotels in einer Stadt, in welche bereits ein Bahn- oder Flugticket gekauft wurde. Problematischer wird es, wenn Personen aufgrund der für sie errechneten Persönlichkeitsprofile Leistungen grundsätzlich nur teurer angeboten bekommen oder von ihnen gänzlich ausgeschlossen werden, es also zu direkter Preisdiskriminierung kommt.[189] Im Bereich von Medikamenten kann es – in hypothetischer Abwesenheit einer festen Preisbindung – gar zu der Situation kommen, dass das (Weiter-)Leben von der Bereitschaft abhängig gemacht wird, den individuell maximal finanzierbaren Preis zu bezahlen. Individual Pricing kann sich in dieser Konstellation dann sogar in die Nähe der Erpressung bewegen. Anders als im gegenwärtigen System wären Unternehmen nicht mehr darauf angewiesen, einen Gleichgewichtspreis anzustreben, sondern könnten bestehende Zwangslagen von Individuen weitgehend ausnutzen. Die einzige Kontrolle würden Wettbewerber darstellen, die aber ihrerseits an einer Gewinnmaximierung interessiert sind und ein Produkt daher wohl kaum signifikant viel günstiger anbieten würden, wenn auch sie um die Zwangslage wissen.

---

187 *Riefa/Markou*, Online Marketing, in: Savin/Trzaskowski (Hrsg.) Research Handbook on EU Internet Law, S. 400.

188 *Riefa/Markou*, Online Marketing, in: Savin/Trzaskowski (Hrsg.) Research Handbook on EU Internet Law, S. 400; *Sandfuchs*, Privatheit wider Willen, S. 23; *Newman*, 40 William Mitchell L. Rev., 849 (867 ff.), 2013-2014.

189 *Riefa/Markou*, Online Marketing, in: Savin/Trzaskowski (Hrsg.) Research Handbook on EU Internet Law, S. 400 m.w.N.; vgl. auch *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 36 f.

Zuletzt kann Individual Pricing auch ein wettbewerbsrechtliches Problem darstellen, indem es kleinere und neuere Wettbewerber in einem Markt systematisch benachteiligt. Wenn sich Individual Pricing auf einer breiten Basis durchsetzt, bedeutet dies im Grundsatz die höchsten Gewinne für die Unternehmen, die die Zahlungsbereitschaft ihrer individuellen Kunden am besten einschätzen können.[190] Bevorzugt werden also zum einen die Unternehmen, die bereits selbst über erhebliche Informationen über diese Kunden verfügen, beispielsweise Facebook, Google und Amazon. Zum anderen profitieren die Unternehmen, die es sich leisten können, entsprechende Persönlichkeitsprofile einzukaufen bei Unternehmen, die auf deren Erstellung und Verkauf spezialisiert sind, beispielsweise das Unternehmen Acxiom[191] oder jedenfalls potentiell auch Facebook selbst. Kleinere Wettbewerber, die diese Ressourcen nicht aufbringen können, sähen sich massiven Wettbewerbsnachteilen ausgesetzt, indem sie weiterhin traditionelle Gleichgewichtspreise mit geringerer Produzentenrente anbieten müssten. Es wäre für sie damit deutlich schwieriger, sich am Markt zu etablieren.

Das durch ausführliche Persönlichkeitsprofile individueller Nutzer ermöglichte Individual Pricing wirft somit in vielerlei Hinsicht ernste Probleme auf, die zeitnah einer Antwort insbesondere durch die Politik und den Gesetzgeber bedürfen, an dieser Stelle aber nicht mehr weiter vertieft werden sollen.

v) Politische Beeinflussung

Eine letzte Verwendungsmöglichkeit der unter anderem in sozialen Netzwerken erstellten detaillierten Persönlichkeitsprofile betrifft mögliche Beeinflussungen politischer Wahrnehmung und Wahlen. Hierzu gibt es noch verhältnismäßig wenig gesicherte Daten, so dass diese Richtung der Verwendung etwas spekulativ bleibt.[192]

Festhalten lässt sich jedenfalls, dass politische Parteien auf einer gewissen Ebene ebenso Werbetreibende sind wie konsumorientierte Unternehmen. Ihre „Produkte“ sind das politische Programm, für das sie stehen, sowie ihre Spitzenkandidaten, mit denen sie zur Wahl antreten. Im Wahlkampf stehen sie im Wettbewerb zu den anderen Parteien um die Stimmen der Wähler. Neben den sicheren Stammwählern versuchen sie vor allem, sich die Stimmen noch unentschiedener Wähler, sowie der Wechselwähler und bisherige Nichtwähler zu sichern.

---

190 *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 16 f.; vgl. auch *Newman*, 40 William Mitchell L. Rev., 849 (870 ff.), 2013-2014.

191 http://www.acxiom.com/; *Pariser*, Filter Bubble, S. 42. ff.

192 Vgl. auch *Chmelik*, Social Network Sites, S. 221 ff.

Hierfür ist der Einsatz von Werberessourcen erforderlich, etwa in Form von Wahlveranstaltungen, Infoständen oder Hausbesuchen bei möglichen Wählern. Gerade die letzte Variante wurde in den USA insbesondere im Präsidentschaftswahlkampf von 2012 praktiziert.[193] Es liegt auf der Hand, dass eine solche individualisierte Ansprache potentielle Wähler umso erfolgsversprechender ist, je mehr über diese individuell bekannt ist.[194] Zum einen können bereits erhebliche Ressourcen eingespart werden, da nicht an jeder Haustür in einer Nachbarschaft geklingelt werden muss, sondern gezielt nur an solchen, in denen der Partei entsprechende Interessen zu erwarten sind. Zudem kann die Ansprache der potentiellen Wähler gezielter und möglicherweise auch manipulativer erfolgen, wenn bekannt ist, was die Wünsche und Hoffnungen dieser individuellen Personen sind. Ein Parteiprogramm kann auf diese Art sehr viel individueller präsentiert werden als dies im Rahmen einer Massenveranstaltung möglich ist.[195]

Soweit hierdurch mehr Wähler überzeugt werden können, kann die umfassende Personalisierung durch soziale Netzwerke die Gewährleistungen des Grundsatzes der Chancengleichheit der Parteien aus Art. 21 Abs. 1 GG i.V.m. Art. 3 Abs. 1 GG beeinträchtigen. Die Möglichkeiten der Wahlwerbung würden in diesem Fall nämlich maßgeblich davon beeinflusst, wie viele Informationen über potentielle Wähler bei den jeweiligen Parteien vorhanden sind. Dies könnte tendenziell größeren Parteien, die vielleicht einen einfacheren Zugang zu entsprechenden Daten erhalten können – nicht zuletzt aufgrund größerer Summen in der Wahlkampfkasse –, wesentliche Vorteile gegenüber kleineren Parteien sichern.

Ein entsprechender Effekt, der beweist, dass derartige Überlegungen durchaus realistisch sind, ließ sich bei der US-Präsidentschaftswahl im Jahr 2012 beobachten. Gerade die Demokraten mit dem Spitzenkandidaten Barack Obama setzten großflächig auf personalisierte Wahlwerbung und individuelle Ansprache von Wählern über das Internet und zu Hause.[196] Dieses Vorgehen stellte eine Weiterentwicklung der Kampagnenstrategie von 2008 dar, in welchem soziale Netzwerke massiv zur Mobilisierung und Ansprache von Freiwilligen sowie

---

193 *Richter*, DÖV 2013, 961 (962); *Weichert*, ZD 2013, 251 (254); vgl. auch *Martini/Fritzsche*, VerwArch (104) 2013, 449 (454).

194 Vgl. *Pariser*, Filter Bubble, S. 152 f.; *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 95 f.

195 *Richter*, Big Data und Demokratische Willensbildung, in: ders. (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 58 f.

196 Ausführlich mit zahlreichen weiteren Nachweisen: *Richter*, DÖV 2013, 961 (961 f.); *Sifry*, How Obama's data-crunching prowess may get him re-elected, http://edition.cnn.com/2011/10/09/tech/innovation/obama-data-crunching-election/index.html.

zum Fundraising eingesetzt wurden.[197] Die personalisierte Analyse und Ansprache von Wählern soll insofern im knappen Rennen um die Präsidentschaftswahl 2012 wahlentscheidende Einflüsse gehabt haben.[198]

Über Effekte im Rahmen der Wahlwerbung hinaus kann und sollte natürlich auch darüber nachgedacht werden, inwieweit die oben beschriebene Filterblase sich allgemein auf politische Überzeugungen auswirken kann. Es ist liegt jedenfalls nicht außerhalb des Vorstellbaren, dass sie nicht nur bestehende politische Überzeugungen verfestigt, sondern sich bei einer entsprechenden Programmierung auch dazu einsetzen ließe, politische Überzeugungen gezielt zu manipulieren.[199] Ob dem so ist, kann an dieser Stelle nicht weiter geklärt werden, sondern bedarf eingehender Forschung insbesondere der Soziologie, Politologie und Informatik. Angesichts der potentiell gravierenden Auswirkungen auf das demokratische System müsste das Recht aber natürlich Regelungen finden, sollten sich derartige Manipulationen nachweisen lassen.

cc) Zwischenfazit: Potentiale privater Datenauswertung und Profilbildung

Facebook im Besonderen aber auch soziale Netzwerke im Allgemeinen erstellen detaillierte Persönlichkeitsprofile ihrer Nutzer. Wie gezeigt wurde, wird nur ein Bruchteil der Daten und Informationen tatsächlich bewusst von Nutzern zur Verfügung gestellt. Ein sehr viel größerer Teil wird abseits ihrer unmittelbaren Kontrolle erhoben und aus Abgleich mit größeren statistischen Mustern gewonnen. Von besonderer Relevanz ist in diesem Zusammenhang die Reichweitenanalyse durch Social PlugIns und Cookies weit über das soziale Netzwerk hinaus.

Die Verwendungsmöglichkeiten der Daten beschränken sich mitnichten auf die Zurverfügungstellung von etwas passenderer Werbung. Die Persönlichkeitsprofile schaffen vielmehr erhebliche Risiken für die Ausübung persönlicher Freiheiten von Nutzern mit teilweise sogar gesamtgesellschaftlichen Konsequenzen.

---

197 *Bieber*, Soziale Netzwerke als neue Arena politischer Kommunikation, in: Bieber u.a. (Hrsg.) Soziale Netzwerke in der digitalen Welt, S. 57 f.

198 *Romano*, Obama's Data Advantage, http://www.politico.com/news/stories/0612/77213.html; *Richter*, Big Data und Demokratische Willensbildung, in: ders. (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 58.

199 Vgl. hierzu *Pariser*, Filter Bubble, S. 141 ff.; *Sandfuchs*, Privatheit wider Willen, S. 46 ff.; *Richter*, Big Data und Demokratische Willensbildung, in: ders. (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 58 ff.; *Chmelik*, Social Network Sites, S. 221 ff.; *Hoffmann-Riem*, Innovation und Recht, S. 633; vgl. allgemein zur Bedeutung von Privatheit und Datenschutz für eine funktionierende Demokratie *Boehme-Neßler*, DVBl. 2015, 1282 (1286 f.); *Mayer-Schönberger*, Die Tugend des Vergessens, S. 129 ff.

Die in gewissem Umfang notwendige Filterung von Inhalten innerhalb des sozialen Netzwerks führt aufgrund ihrer aktuellen intransparenten Ausgestaltung zur Formung einer Filterblase, mit der möglichen Folge einer intellektuellen und sozialen Verarmung der Nutzer. Zudem können durch die Persönlichkeitsprofile wirtschaftliche Teilhabechancen beeinträchtigt werden. Im Zusammenhang mit Risikoprognosen und Individual Pricing können bestimmte Leistungen für einzelne Personen nur zu erschwerten Bedingungen zugänglich gemacht oder gänzlich verweigert werden. Indem die Profilbildung außerhalb der Kontrolle des Individuums liegt und häufig auf statistischen Zuordnungen beruhen, bestehen in solchen Fällen nur wenige Einspruchs- und Korrekturmöglichkeiten. Zuletzt kommt es zu einer Fragmentierung und Privatisierung des öffentlichen Raums, indem viel Kommunikation und Interaktion gemäß den Algorithmen des privaten Akteurs Facebook stattfindet.

Keines dieser Probleme rechtfertigt die Forderung nach einem Verbot sozialer Netzwerke oder ihre generelle Verteufelung. Es ist unbestritten, dass sie den Alltag vieler Nutzer erleichtern und sich daher auch zu Recht einer großen Beliebtheit erfreuen. Die Probleme weisen aber darauf hin, dass es sich bei sozialen Netzwerken zum einem gewissen Grad um eine Risikotechnologie handelt, die entsprechend staatlicher Regulierung bedarf. Ein wesentlicher Baustein hierfür ist das Datenschutzrecht, welches im Fokus der rechtlichen Betrachtung dieser Arbeit steht.

III. Staatlicher Zugriff auf die Daten sozialer Netzwerke

Die in sozialen Netzwerken gespeicherten Daten und ihr Potential für umfassende Profilbildungen wecken auch staatliche Begehrlichkeiten. Sowohl für polizeiliche Ermittlungsbehörden als insbesondere auch Nachrichtendienste bieten sie wichtige Ermittlungsmöglichkeiten.[200] Seit dem 11. September 2001 ist eine erhebliche Zunahme an staatlichen gesetzlichen Auskunftsansprüchen und Überwachsungsrechten zu beobachten gewesen. Diese Auskunftsrechte beziehen sich insbesondere auf sogenannte Metadaten der Kommunikation, also die technischen Verbindungsdaten, die Aufschluss darüber geben, wer wann mit wem an welchem Ort wie lange kommuniziert hat. Betroffen sind sowohl die USA,

[200] Ausführlich: *Martini*, VerwArch (107) 2016, 307 (308 ff.); *Singelnstein*¸ NStZ 2012, 593 (599 f.).

in denen die Daten vieler sozialer Netzwerke gespeichert werden, als auch Mitgliedsstaaten der Europäischen Union, nicht zuletzt Deutschland.[201]

Dass Legislative und Exekutive hier aktuell zu einer Überbetonung der Sicherheitsaspekte zulasten individueller Freiheitsrechte tendieren, legen zahlreiche Entscheidungen der Judikativen dies- und jenseits des Atlantiks dar, welche Gesetzgebungsvorhaben aufgrund einer übermäßigen Einschränkung von Freiheitsrechten für jedenfalls teilweise rechtswidrig erklärt haben.[202]

Staatliche Datenverarbeitung kann erhebliche Eingriffe in die Freiheitsrechte Betroffener bedeuten, was nicht zuletzt das Bundesverfassungsgericht bereits 1983 unter Anführung der heute als *chilling effects* bekannten Abschreckungseffekte im Volkszählungsurteil feststellte.[203] Durch das staatliche Gewaltmonopol können negativ von der staatlichen Ordnung Abweichende mit Sanktionen belegt werden. Der Staat kann sein Wissen einsetzen, um eigene Wertvorstellungen durchzusetzen und es dabei gegebenenfalls sogar missbrauchen.[204]

Im Folgenden soll ein kurzer Überblick darüber gegeben werden, inwiefern staatliche Stellen auf soziale Netzwerke zugreifen können und dies aktuell tun. Hierbei wird kein Anspruch auf Vollständigkeit erhoben. Im Anschluss wird das Gefährdungspotential staatlicher und privater

---

201 Für eine ausführliche Darstellung vgl. *Buchner*, Informationelle Selbstbestimmung, S. 68 ff.; *Kipker*, Informationelle Freiheit und staatliche Sicherheit, S.11 ff.; vgl. auch *Mayer-Schönberger*, Die Tugend des Vergessens, S. 189 ff.

202 Vgl. beispielsweise die Entscheidungen des BVerfG zum zum Großen Lauschangriff 2004 (BVerfGE 109, 279 ff.), zur Rasterfahndung 2006 (BVerfGE 115, 320 ff.) und zur Online-Durchsuchung 2008 (BVerfGE 120, 274 (345)), sowie die Urteile zur Unvereinbarkeit wesentlicher Aspekte einer Vorratsdatenspeicherung sowohl mit nationalen als auch europäischen Grundrechten (BVerfGE 120, 274 ff.; EuGH, Rs. C-293/12 = DVBl. 2014, 708 ff.). Auch in den USA entschied im Mai 2015 ein Bundesgericht in zweiter Instanz, dass die anlasslose Überwachung und Sammlung von Telefon-Metadaten nicht durch § 215 des Patriot Acts gerechtfertigt sei und dieser im Übrigen einem vollständigen judical review unterläge – anders als dies bisher von den Sicherheitsbehörden angenommen wurde, United States Court of Appeals for the second circuit, *ACLU v. Clapper*, entschieden am 7.5.2015, No. 14-42-cv, abrufbar unter http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf, S. 2. Zuvor hatte bereits ein Bundesgericht in einem anderen Fall (*Klayman v. Obama*) in erster Instanz in die Rechtmäßigkeit der anlasslosen Massenüberwachung von Internet- und Telefonmetadaten in den USA in Frage gestellt, United States District Court for the District of Columbia, *Klayman v. Obama*, entschieden am 16.12.2013, No. 13-0851 u. 13-0881, abrufbar unter https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48, S. 5 f. Diese Entscheidung wurde indes in zweiter Instanz aufgehoben und zurückverwiesen, da insbesondere keine hinreichende Verletzung eigener subjektiver öffentlicher Rechte der Kläger dargelegt worden sei, United States Court of Appeals for the District of Columbia, *Klayman v. Obama*, entschieden am 28.8.2015, No. 14.5004, abrufbar unter http://www.cadc.uscourts.gov/internet/opinions.nsf/ED64DC482F286F1785257EAF004F71E8/$file/14-5004-1570210.pdf, S. 7 ff.; vgl. für einen Überblick der Rechtsprechung des EuGH zum Datenschutz *Skouris*, NVwZ 2016, 1359 (1359 ff.).

203 BVerfG, 63, 1 (42 f.) – Volkszählungsurteil; *Kipker*, Informationelle Freiheit und staatliche Sicherheit, S. 68 f.; vgl. auch *Oermann/Staben*, Der Staat (52) 2013, S. 640 ff.; *Das/Kramer*, Self-Censorship on Facebook, http://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350, S. 120, 125.

204 *Buchner*, Informationelle Selbstbestimmung, S. 68.

Datenverarbeitung gegenübergestellt. Das geltende nationale deutsche Datenschutzrecht unterscheidet zwischen öffentlicher und nicht-öffentlicher Datenverarbeitung. Dies wird verbreitet mit der Prämisse begründet, dass staatliche Datenverarbeitung eine größere Bedrohung für den Betroffenen darstellt als private Datenverarbeitung.[205] Es soll gezeigt werden, dass diese Prämisse heute nicht mehr uneingeschränkt gilt, ohne dass damit aber ein Plädoyer für ein einheitliches Datenschutzrecht einhergehen soll.[206]

1. Zugriff durch Ermittlungsbehörden

Soziale Netzwerke enthalten überaus sensible Informationen über ihre Nutzer und bieten somit auch dem Staat – insbesondere seinen Ermittlungsbehörden – Informationsmöglichkeiten. Diese betreffen zum einen die Informationsbeschaffung, zum anderen aber auch die Informationsverbreitung.[207]

Speziell bei der Ermittlungsarbeit der Polizei ist zunächst zwischen einer bloßen Internetaufklärung, bei der öffentlich zugängliche Informationen zur Kenntnis genommen und ausgewertet werden, und verdeckten Ermittlungen zu unterscheiden.[208] Die Auswertung öffentlich zugänglicher Informationen ist nach herrschender Ansicht von den polizeilichen Generalklauseln der §§ 161, 163 StPO, bzw. §§ 7, 20b BKAG gedeckt.[209] Die entscheidende tatbestandliche Frage ist freilich, wann Informationen als öffentlich zugänglich einzustufen sind. Regelmäßig wird dies nur dann zu bejahen sein, wenn keine relevanten Zugangshürden zu überwinden sind. Die in sozialen Netzwerken, speziell bei Facebook bestehende Registrierungspflicht wird zurecht nicht als solche Hürde eingestuft, da keine Überprüfung der angegebenen Personalien stattfindet und die Registrierung daher ohne Aufwand möglich ist.[210] Dagegen sind Daten, die nur „Freunden“ zugänglich gemacht werden, deren Sichtbarkeit also von einer Bestätigung einer Kontaktanfrage durch den individuellen Nutzer abhängt, als nicht-

---

205 Vgl. *Buchner*, Informationelle Selbstbestimmung, S. 76 f.; *Masing*, NJW 2012, 2305 (2309).

206 Ausführlich zur Differenzierung des Datenschutzrechts in einen öffentlichen und nicht-öffentlichen Teil *Kühling*, Die Verwaltung (44) 2011, 523 (548 ff.).

207 Ausführlich: *Martini*, VerwArch (107) 2016, 307 (308 ff.).

208 Instruktiv: *Soiné*, NStZ 2014, 248 (248 ff.); *Weichert*, JBÖS 2012/2013, S. 381 ff.; *Rosengarten/Römer*, NJW 2012, 1764 (1764 ff.).

209 *Singelnstein*, NStZ 2012, 593 (600); Weichert, JBÖS 2012/2013, S. 384 f.; *Rosengarten/Römer*, NJW 2012, 1764 (1764); *Schulz/Hoffmann*, CR 2010, 131 (136); *Kölbel*, in: MüKo-StPO, Bd. 2, § 161 StPO, Rn. 11 m.w.N.; a.A. *Oermann/Staben*, Der Staat 52 (2013), S. 659 f., da es sich aufgrund der damit verbundenen Abschreckungswirkung um einen erheblichen mittelbaren Eingriff in die Grundrechte der Betroffenen handele und somit eine gesonderte Ermächtigungsgrundlage erforderlich sei.

210 *Kölbel*, in: MüKo-StPO, Bd. 2, § 161 StPO, Rn. 11 m.w.N.; vgl. zur allgemeinen Zugänglichkeit auch *Taeger* , in: Taeger/Gabel, § 28 BDSG, Rn. 83.

öffentlich einzustufen.[211] Selbst die strengsten Privatsphäreeinstellungen bei Facebook gestatten es nicht, den Namen und das Profilfoto vor allen Nutzern zu verbergen; diese Daten sind somit stets als öffentlich anzusehen. Polizeilich genutzt werden sie unter anderem zur Identifizierung von Fahrzeugführern bei Geschwindigkeitsübertretungen oder anderen Verkehrsverstößen.[212]

Problematischer ist der Einsatz von verdeckten Ermittlern, die unter einer Legende auftreten und Nutzern damit eine falsche Identität vorspiegeln. Freilich besteht im Internet kein grundsätzlich schutzwürdiges Vertrauen in die Identität eines Kommunikationspartners, so dass nicht jede Täuschung einen Grundrechtseingriff darstellt.[213] Soziale Netzwerke zeichnen sich allerdings durch eine gewisse Langfristigkeit der Kontaktpflege aus. Zudem bilden sie häufig real bestehende soziale Beziehungen nach, da Kontaktanfragen gezielt beantwortet und hierdurch Zugangshürden für die Datenteilung aufgestellt werden. Sie schaffen damit eine Atmosphäre, in der regelmäßig ein gewisser Vertrauensschutz hinsichtlich der Identität anderer Mitglieder suggeriert wird.[214] Insbesondere Facebook statuiert sogar in seinen Nutzungsbedingungen unter Punkt 4.1 eine Pflicht, auch anderen Nutzern gegenüber nur unter dem echten Namen aufzutreten.[215] Während dieser Klarnamenzwang zwar in Deutschland gegen das Recht auf anonyme bzw. pseudonyme Nutzung aus § 13 Abs. 6 TMG verstößt und damit zumindest anderen Nutzern gegenüber als rechtswidrig einzustufen ist[216], suggeriert er zumindest – solange er von Facebook dennoch durchgesetzt wird – ein gegenüber dem restlichen Internet erhöhtes Vertrauen in die Identität von Kommunikationspartnern. Entsprechend sind verdeckte Ermittlungen in sozialen Netzwerken nur unter den restriktiven Voraussetzungen der §§ 110a, 110b StPO zulässig.[217] Der Zugriff von polizeilichen Ermittlungsbehörden auf personenbezogene Daten in sozialen Netzwerken unterliegt damit strengen Voraussetzungen.

Weitere Ermittlungsmöglichkeiten eröffnen sich für Polizeibehörden durch die Analyse von Beziehungsgeflechten in sozialen Netzwerken und Abgleich mit verschiedensten verfügbaren

---

211 *Weichert*, JBÖS 2012/2013, S. 385.
212 *Weichert*, JBÖS 2012/2013, S. 385.
213 So ausdrücklich BVerfGE 120, 274, 345 – Onlinedurchsuchung = NJW 2008, 822, 836 Rn. 311; kritisch: *Singelnstein*, NStZ 2012, 593 (600); *Schulz/Hoffmann*, CR 2010, 131 (133).
214 *Weichert*, JBÖS 2012/2013, S. 386; *Rosengarten/Römer*, NJW 2012, 1764 (1766 f.); *Martini*, VerwArch (107) 2016, 307 (322 ff.).
215 https://www.facebook.com/legal/terms?ref=pf (Stand 30. Januar 2015).
216 Hierzu ausführlich unten unter D.II.2.b).
217 *Soiné*, NStZ 2014, 248 (250); *Singelnstein*, NStZ 2012, 593 (600); *Weichert*, JBÖS 2012/2013, 379 (387 f.); *Rosengarten/Römer*, NJW 2012, 1764 (1767).

Daten im Rahmen von Big Data Analysen.[218] Vor allem in den USA stellt das *predictive policing* mittlerweile einen festen Bestandteil der modernen Polizeiarbeit dar.[219] Hierbei wird basierend auf statistischen Analysen berechnet, an welchen Orten oder durch welche Personen mit einer erhöhten Wahrscheinlichkeit mit Straftaten zu rechnen ist und entsprechend eine verstärkte Polizeipräsenz bereitgestellt. Mögliche Missbrauchsmöglichkeiten in Form von Vorverurteilungen von Individuen aufgrund statistischer Berechnungen liegen auf der Hand und unterstreichen die Notwendigkeit einer rechtlichen Regulierung.[220]

Auch für Steuerfahndungsbehörden können die in sozialen Netzwerken verfügbaren Daten relevant sein, indem sie beispielsweise Aufschluss über Vermögenswerte geben.[221] Jedenfalls wenn es sich hierbei um die Zusammenführung verschiedenster Daten im Rahmen von Big Data Analysen handelt, ist eine solche Analyse zwar technisch aussichtsreich; inwieweit dies von hinreichenden Ermächtigungsgrundlagen gedeckt ist, ist aber stets im Einzelfall kritisch zu prüfen.[222]

Wegen ihrer hohen Reichweite werden soziale Netzwerke auch zunehmend zur Verbreitung von behördlichen Informationen genutzt. Dies geschieht insbesondere mittels sogenannter „Fanpages“. Einsatzbereiche sind sowohl die Kommunikation mit Bürgern im Rahmen eines Bürgerdialogs, als auch Fahndungsaufrufe der Polizei.[223] Die hierbei auftretenden Probleme und die grundsätzliche Zulässigkeit einer derartigen staatlichen Nutzung von sozialen Netzwerken sind bisher nur wenig erforscht und sollen unten unter D.I.3.c)dd) näher untersucht werden.

2. Zugriff durch Nachrichtendienste

Nicht zuletzt die NSA-Affäre und die Enthüllungen durch Edward Snowden haben den Zugriff von Nachrichtendiensten auf personenbezogene Daten im Internet im Allgemeinen und sozialen Netzwerken im Besonderen verstärkt in das Bewusstsein der Öffentlichkeit gebracht. Nach den bekannt gewordenen Informationen ist davon auszugehen, dass Sicherheitsbehörden der USA, insbesondere die NSA und das FBI, sowie ihre Partnerdienste wie der britische

218 *Martini*, DVBl. 2014, 1481 (1481 f.).
219 *Martini*, DVBl. 2014, 1481 (1481) m.w.N.; ausführlich zum Problem der Kriminalisierung durch Datenverarbeitung *Kipker*, Informationelle Freiheit und staatliche Sicherheit, S. 38 ff.
220 Hierzu ausführlich *Martini*, DVBl. 2014, 1481 (1488 f.).
221 So auch *Martini*, VerwArch (107) 2016, 307.
222 Ausführlich *Martini*, VerwArch (107) 2016, 307 (321 ff.); vgl. auch *Weichert*, JBÖS 2012/2013, 379 (390).
223 Instruktiv: *Caspar*, ZD 2015, 12 (12 ff.); *Weichert*, JBÖS 2012/2013, 379 (381 ff.).

GCHQ Zugriff auf die gespeicherten Daten amerikanischer sozialer Netzwerke haben.[224] Ein spezifischer Anfangsverdacht muss hierbei nicht vorliegen. Vielmehr kann die NSA u.a. im Rahmen des PRISM-Programms anlasslos und unbeschränkt auf alle Daten zugreifen, die auf amerikanischen Servern gespeichert sind.[225] Dies betrifft in besonderem Maße die von den großen amerikanischen sozialen Netzwerken erhobenen und gespeicherten Daten, insbesondere von Facebook, da diese jedenfalls teilweise auf Servern der Facebook Inc. in den USA gespeichert werden.[226] Wegen bestehender Kooperationsabkommen von der NSA mit anderen nationalen Geheimdiensten, nicht zuletzt dem BND, ist darüber hinaus nicht ausgeschlossen, dass die so gewonnenen Daten, gegebenenfalls in Umgehung rechtlicher Beschränkungen für die eigenhändige Erhebung, auch in die Hände deutscher Nachrichtendienste gelangen.[227]

Ein solch umfassender nachrichtendienstlicher Zugriff ist als schwerwiegende Verletzung der informationellen Selbstbestimmung der Betroffenen zu werten, da diese hierüber nicht informiert werden und über den Umfang daher allenfalls mutmaßen können.[228] Der Empfehlung des Generalanwalts folgend hat der EuGH daher im Oktober 2015 das Safe-Harbor Abkommen mit den USA[229] für ungültig erklärt, da in den USA kein angemessenes Datenschutzniveau im Sinne von Art. 25 DSRL vorliege.[230] Zudem stellte der EuGH ausdrücklich fest, dass nationalen Datenschutzaufsichtsbehörden eine Kompetenz zukommt, die Rechtmäßigkeit eines Datentransfers zu überprüfen und diesen gegebenenfalls zu untersagen.[231] Ob das nunmehr im Juli 2016 in Kraft getretene Nachfolgeabkommen zwischen der EU und den USA, der sogenannte „EU-US Privacy Shield“, tatsächlich den Anforderungen genügt, die durch den EuGH aufgestellt wurden, wird bezweifelt, wenngleich die Kommission durchaus bemüht war, diese umzusetzen.[232] Eine ausführliche Untersuchung muss an dieser

---

224 Schlussanträge des Generalanwalts *Bot*, v. 23.9.2015, Rs. C-362/14, Rn. 155 ff.; vgl. auch *Plath*, in: Plath, § 11 BDSG, Rn. 54; *Maisch*, Informationelle Selbstbestimmung, S. 196 f.

225 Schlussanträge des Generalanwalts *Bot*, v. 23.9.2015, Rs. C-362/14, Rn. 26, 153.

226 Schlussanträge des Generalanwalts *Bot*, v. 23.9.2015, Rs. C-362/14, Rn. 24; vgl. auch *Plath*, in: Plath, § 11 BDSG, Rn. 54.

227 *Petri*, ZD 2013, 557 (560).

228 Schlussanträge des Generalanwalts *Bot*, v. 23.9.2015, Rs. C-362/14, Rn. 172; vgl. für eine Analyse der abschreckenden Effekte und den daraus resultierenden Grundrechtsbeeinträchtigungen: *Oermann/Staben*, Der Staat (52) 2013, 630 (644 f.); ausführlich zu den verletzten Grundrechten und den Schutzmöglichkeiten gegenüber staatlichen Spähangriffen: *Hoffmann-Riem*, Innovation und Recht, S. 675 ff.

229 Entscheidung der Kommission 2000/520/EG v. 26.7.2000.

230 EuGH, *Schrems v. Data Protection Commisioner*, Rs. C-362/14, Rn. 98, 106 = ZD 2015, 549 (555); Schlussanträge des Generalanwalts, *Bot*, v. 23.9.2015, Rs. C-362/14, Rn. 183, 237.

231 EuGH, *Schrems v. Data Protection Commisioner*, Rs. C-362/14, Rn. 63 ff. = ZD 2015, 549 (552); entsprechend hat mittlerweile der Irish High Court die irische Datenschutzbehörde angewiesen, eine ausführliche Überprüfung des Datentransfers in die USA durch Facebook vorzunehmen, vgl. http://www.europe-v-facebook.org/MU_HC.pdf.

232 Ausführlich hierzu *Weichert*, ZD 2016, 209 (214 ff.); *Schreiber/Kohm*, ZD 2016, 255 (257 ff.).

Stelle allerdings der weiteren Forschung und gegebenenfalls erneut der Entscheidung des EuGH überlassen bleiben.

Es liegt in der Natur der Sache geheimdienstlicher Arbeit, dass sie nach außen nicht transparent ist und auch im Vorfeld eines konkreten Anfangsverdachtes geschehen kann. Umso wichtiger sind eine gesetzliche Beschränkung geheimdienstlicher Befugnisse und die effektive Kontrolle der Einhaltung dieser Beschränkungen etwa durch parlamentarische Gremien.[233] Das generell im Datenschutzrecht geltende Verbot mit Erlaubnisvorbehalt für die Datenverarbeitung findet grundsätzlich auch gegenüber den Nachrichtendiensten Anwendung. Gesetzliche Erlaubnisvorschriften für die Verarbeitung personenbezogener Daten finden sich in Deutschland insoweit u.a. in den Gesetzen der einzelnen Nachrichtendienste, insbesondere dem BVerfSchG, dem BNDG und dem MADG, sowie dem Artikel 10 Gesetz (G10). Darüber hinaus statuieren Normen des TKG und des TMG Auskunfts- und Übermittlungspflichten der Anbieter von Telekommunikation und Telemedien gegenüber bzw. an staatliche Stellen, insbesondere auch Nachrichtendienste.[234] Die im Rahmen der NSA-Affäre bekannt gewordenen Praktiken und die schleppende Aufklärung im Rahmen des einberufenen Untersuchungsausschusses werfen allerdings Zweifel daran auf, ob diese Vorgaben immer eingehalten worden sind.

In diesem Zusammenhang wird geltend gemacht, dass massenhafte nachrichtendienstliche Zugriffe auf soziale Netzwerke eine erhöhte Sicherheit bieten können, indem Terroristen frühzeitig enttarnt werden. Tatsächlich sind bisher aber kaum große empirische Erfolge der NSA oder des BND bekannt. Dies mag zwar zum Teil in der Natur der Sache liegen, verwundert angesichts des langen Zeitraums, in welchem die verstärkte Überwachung bereits praktiziert wird, aber dennoch.[235] Vielmehr stellt es eine Gefährdung des allgemeinen Persönlichkeitsrechts, insbesondere der informationellen Selbstbestimmung, durch den Abschreckungseffekt aber auch der Meinungsfreiheit dar, dass ein nahezu ungehinderter Zugriff amerikanischer Dienste auf in den USA gespeicherte Daten möglich ist. Angesichts der geringen empirischen Erfolge und der Schwere des grundrechtlichen Eingriffs ist daher dem EuGH ebenso wie dem Generalanwalt *Bot* darin beizupflichten, dass ein solcher Zugriff in

233 Vgl. *Petri*, ZD 2013, 557 (561).

234 Instruktiv: *Englerth/Hermstrüwer*, RW 2013, 326 (339 ff., 351 ff.).

235 *Petri*, ZD 2013, 557 (558) führt an, dass die NSA zunächst angab, bis 2013 immerhin 54 Terroranschläge durch Maßnahmen jahrelanger Massenüberwachung der gesamten Telekommunikation verhindert zu haben. Im Rahmen einer Ausschussanhörung des US-Senats mussten diese Zahlen indes auf zwölf Fälle hinunter korrigiert werden. Deutschland soll bis 2013 in zwei Fällen von den Überwachungstätigkeiten der NSA profitiert haben.

keiner Weise mit europäischen Grundrechten vereinbar ist und sogar ihren „Wesensgehalt" verletzt.[236]

3. Freiheitsbeschränkendes Potential staatlicher vs. privater Datenverarbeitung

Anders als teilweise in der Literatur vertreten wird, ist staatliche Datenverarbeitung nicht als grundsätzlich bedrohlicher für die individuelle Freiheit einzustufen als kommerzielle private Datenverarbeitung.[237] Vielmehr können sowohl der Staat als auch private Akteure eigene Agenden verfolgen, die sie mit Hilfe der ihnen zur Verfügung stehenden Daten und wirksamen Zwangsmitteln durchzusetzen versuchen.

a) Zwecke der Beeinflussung

Natürlich ist zunächst nur der Staat auf die Schaffung und Einhaltung gewisser Wertvorstellungen in der Gesellschaft – etwa in Form von Gesetzen – ausgerichtet, während private Akteure primär Geld verdienen wollen. Private Akteure sind aber mitnichten „weitgehend unvoreingenommen und wertfrei"[238]. Es ist zwar richtig, dass sich beispielsweise auch mit unzuverlässigen Kunden durch bestimmte Dienstleistungen Geld verdienen lässt, wenn sich die Dienstleister nur hinreichend an ihre Kunden anpassen.[239] Der Gedanke, dass privaten Dienstleistern weniger daran gelegen ist, das Verhalten oder bestimmte Eigenschaften individueller Verbraucher zu beeinflussen und mehr daran, sich an diese anzupassen, dürfte indes eher in den Grenzen ihrer traditionellen Möglichkeiten begründet liegen. Einzelne Unternehmen hatten in der Vergangenheit weder die Macht noch die Informationen, die notwendig gewesen wären, das Verhalten einzelner Kunden gezielt zu verändern. Dies ändert sich gerade: Wie in den vorigen Abschnitten beschrieben, erlauben detaillierte Persönlichkeitsprofile in Verbindung mit Big Data Analysen sehr präzise Voraussagen über menschliches Verhalten und schaffen somit auch erhebliche Einflussmöglichkeiten.

Buchner verweist zwar zutreffend darauf, dass es „im absoluten Sinne, nicht *den einen* guten oder schlechten Kunden" gibt, da die private Wirtschaft aus zu unterschiedlichen Akteuren mit

---

236 EuGH, *Schrems v. Data Protection Commisioner*, Rs. C-362/14, Rn. 94 f. = ZD 2015, 549 (555); Schlussanträge des Generalanwalts, *Bot*, v. 23.9.2015, Rs. C-362/14, Rn. 171, 183.

237 So aber *Buchner*, Informationelle Selbstbestimmung, S. 68, 130; *Masing*, NJW 2012, 2305 (2309); *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 54 f.; wie hier auch bereits *Hoffmann-Riem*, AöR 1998, 513 (524 f.); vgl. auch *Eichenhofer*, Der Staat (55) 2016, 41 (55); *Gurlit*, NJW 2010, 1035 (1039 f.).

238 So aber *Buchner*, Informationelle Selbstbestimmung, S. 66.

239 *Buchner*, Informationelle Selbstbestimmung, S. 67.

unterschiedlichen Interessen besteht.[240] Diese Analyse verfehlt indes dort das Problem, wo es um einige wenige Marktakteure mit monopolähnlicher oder oligopolistsicher Vormachtstellung geht, wie dies aktuell etwa bei Google, Facebook, Amazon und Apple der Fall ist.[241] Diese Unternehmen dürften nämlich von einer Homogenisierung ihrer Kunden, die größere, vorhersehbarere Absatzmärkte schafft und eine bessere Nutzung von Skaleneffekten ermöglicht, profitieren. Gerade im Falle von Facebook und Google ist eine zu große Individualität der Kunden für die Effektivität des eigenen Geschäftsmodells nicht unbedingt förderlich, da aus Big Data abgeleitete Prognosen hinsichtlich der Effektivität bestimmter Werbung potentiell unzuverlässiger werden. Auch mag für diese Unternehmen die politische Ideologie oder die Religion ihrer Kunden von nachrangiger Bedeutung sein. Sehr vorteilhaft für sie sind indes Kunden, die konsumfreudig, wenig kritisch und wenig nachhaltig sind. Obwohl sicherlich auch andere Kunden bedienet werden, stellen dies Eigenschaften dar, an deren Förderung die Unternehmen ein Interesse haben dürften. Der entscheidende Unterschied zu früheren Unternehmen ist, dass diese Internetmonopolisten auch die Möglichkeiten haben, eine gewisse Beeinflussung ihrer Kunden in diese Richtung zu unternehmen.[242] Apple kann beispielsweise über iTunes nicht unerheblichen Einfluss auf den Musikgeschmack seiner Kunden ausüben und über das regelmäßige Herausbringen neuer Produkte mit geringem Innovationsgehalt Nachhaltigkeitsvorstellungen beeinflussen. Amazon beeinflusst über seine Kaufempfehlungen künftiges Kaufverhalten seiner Kunden in vielen Lebensbereichen. Google und Facebook analysieren ihre Nutzer noch weit darüber hinaus und können durch die Effekte der Filter Bubble, aber auch zielgerichtete Werbung das Verhalten und gegebenenfalls sogar politische Ansichten nachhaltig beeinflussen.[243]

Staatliche und private Akteure haben somit zwar nicht inhaltlich, wohl aber funktional vergleichbare Interessen an einer Beeinflussung und Steuerung von Individuen.

---

240 *Buchner*, Informationelle Selbstbestimmung, S. 66 f.

241 Vgl. *Hoffmann-Riem*, Innovation und Recht, S. 636 ff.; *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 34 ff.; *Buchholtz*, AöR 2015, 121 (126); *Schliesky u.a.*, Schutzpflichten und Drittwirkung im Internet, S. 124, die Betreibern von sozialen Netzwerken und in größerem Kontext auch Suchmaschinenbetreibern und Providern insoweit als „Gatekeeper“ zu dem öffentlichen Raum des Internets bezeichnen.

242 *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 34 ff.

243 Hierzu ausführlich oben unter B.II.3.

b) Sanktionsmechanismen

Funktional vergleichbar sind auch die Sanktionsmechanismen, die staatlichen und privaten Akteuren zur Verfügung stehen, wenn unerwünschtes Verhalten durch die Datenverarbeitung erkennbar wird.

Freilich ist die Möglichkeit des Staates zur exekutiven Sanktion in Form von gerichtlicher Verurteilung und Inhaftierung einzigartig. Diese Möglichkeit stellt indes eine *ultima Ratio* dar, die erst eintritt, wenn tatsächlich ein nachweisbares, strafrechtlich relevantes Fehlverhalten vorliegt. Der strafrechtlichen Sanktion vorgelagert sind dagegen beispielsweise zur Vorbeugung von terroristischen Anschlägen Risikoeinsstufungen aufgrund von Big Data Analysen oder ermittlungsbehördlicher und nachrichtendienstlicher Überwachung. Wie zuvor beschrieben können solche Maßnahmen regelmäßig zu Freiheitseinschränkungen aufgrund von Abschreckungseffekten oder auch ganz konkret einer Eintragung auf den sogenannten „no-fly-lists“ oder Kontensperrungen führen. Durch die Großflächigkeit, mit der solche Überwachung derzeit stattfindet, kann sie immer wieder auch Unschuldige betreffen, insbesondere in Form der Abschreckungseffekte.[244]

Während derartige staatliche Maßnahmen zweifellos einschneidend wirken können, unterschätzt es doch die Sanktionsmöglichkeiten privater Datenverarbeitung, wenn man der staatlichen Datenverarbeitung pauschal ein „wesentlich größeres Druck- und Bedrohungspotential“[245] zuspricht.[246] Der zentrale Sanktionsmechanismus privater Datenverarbeitung ist die Erzeugung eines sozialen und ökonomischen Konformitätsdrucks. Speziell in sozialen Netzwerken können durch die Gestaltung der Nutzungsbedingungen gewisse Umgangsformen und Verhaltensweisen vorgegeben werden; bei Nichtkonformität droht ein Ausschluss. Angesichts der erheblichen Verbreitung von Facebook und anderen sozialen Netzwerken gerade in jüngeren Teilen der Bevölkerung stellt dies eine sehr relevante soziale Form der Sanktionierung dar, die teilweise mit einer erheblichen sozialen Isolation einhergehen kann.[247]

---

244 Vgl. BVerfGE 120, 378 (402) – automatische Kennzeichenerfassung.

245 So *Buchner*, Informationelle Selbstbestimmung, S. 68; vgl. auch *Masing*, NJW 2012, 2305 (2309).

246 Vgl. auch bereits *Schulz*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, § 1 TDDSG, Rn. 18; *Simitis*, in: Simitis, BDSG, § 1 Rn. 45; *Bäcker*, Der Staat (51) 2012, 91 (101); *Greve*, Drittwirkung, in: FS Kloepfer, S. 670 ff.

247 Vgl. *Spiecker gen. Döhmann*, K&R 2012, 717 (720); *Jandt/Roßnagel*, MMR 2011, 637 (637 f.); auch angedeutet von *Sandfuchs*, Privatheit wider Willen, S. 136; *Kutscha*, GR-Schutz im Internet, S. 11 f.; vgl. hierzu im Kontext der Freiwilligkeit der Einwilligung auch unten unter D.III.2.b)cc).

Auf ökonomischer Ebene wird Konformitätsdruck ausgeübt, indem etwa Kredit- oder Versicherungsverträge bei unerwünschtem, von der Norm abweichenden Verhalten teurer werden. Insbesondere für wirtschaftlich schwächer gestellte Nutzer und Kunden kann dies erhebliche Auswirkungen haben. Ferner können Kaufpräferenzen und Wertvorstellungen unterschwellig manipuliert und damit die individuelle Entschließungsfreiheit beeinträchtigt werden.

c) Zwischenfazit

Staatliche und private Datenverarbeitung unterscheiden sich daher vor allem in dem konkreten Zweck der Beeinflussung und den Sanktionsmechanismen, nicht so sehr dagegen in ihrem abstrakten Bedrohungspotential für die individuelle Freiheit. Angesichts der unterschiedlichen Wirkungsmechanismen und auch der unterschiedlichen rechtlichen Stellung – der Staat ist immerhin Grundrechtsverpflichteter, während gegenüber Privaten nur eine mittelbare Drittwirkung existiert[248] – mag es dennoch gerechtfertigt und angemessen sein, den Datenschutz wie bisher in einen öffentlichen und einen nicht-öffentlichen Teil zu gliedern.[249] Hiermit darf aber keinesfalls eine undifferenzierte Relativierung des Gefährdungspotentials privater, insbesondere kommerzieller Datenverarbeitung im Zeitalter von Big Data einhergehen.

Entsprechend liegt der weitere Fokus dieser Arbeit auf den Möglichkeiten des Datenschutzrechts, mit den Herausforderungen umzugehen, die speziell Facebook als maßgeblicher privater Akteur im Bereich der sozialen Netzwerke stellt. Die Gefahren und Probleme, die sich im Zusammenhang von staatlicher Datenverarbeitung und sozialen Netzwerken ergeben, sollen hierdurch keinesfalls relativiert oder verharmlost werden. Vieles ist auch dort unklar, beispielsweise die Frage, unter welchen Voraussetzungen und in welchem Umfang soziale Netzwerk Accounts beschlagnahmt[250] und wann konkret und in welchem Umfang verdeckte Ermittler eingesetzt werden können.[251] Da das Erkenntnisinteresse dieser

248 *Taeger/Schmidt*, in: Taeger/Gabel, Einf BDSG, Rn. 48 f.; *Masing*, NJW 2012, 2305 (2306 ff.); *Bäcker*, Der Staat (51) 2012, 91 (99 ff.); *Greve*, Drittwirkung, in: FS Kloepfer, S. 670 ff.; *Eichenhofer*, Der Staat (55) 2016, 41 (55 ff.).

249 Ausführlich: *Kühling*, Die Verwaltung (44) 2011, 525 (550 f.); *Masing*, NJW 2012, 2305 (2306 ff.); *Rogall-Grothe*, ZRP 2012, 193 (195 f.); *Herrmann*, ZD 2014, 439 (440); *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 190; vgl. auch *Buchholtz*, AöR 2015, 121 (135).

250 Hierzu *Englerth/Hermstrüwer*, RW 2013, 326 (339 ff.).

251 Instruktiv: *Soiné*, NStZ 2014, 248 (249 f.); *Singelnstein*, NStZ 2012, 593 (600); *Weichert*, JBÖS 2012/2013, 379 (387 f.); *Rosengarten/Römer*, NJW 2012, 1764 (1765 ff.).

Arbeit indes auf Aspekten der Regulierung privater Akteure liegt, sollen diese Fragen im Folgenden weitgehend ausgeblendet und der weiteren Forschung überlassen werden.

C. Überblick: Einfachgesetzlicher Datenschutzrahmen sozialer Netzwerke

Datenverarbeitung in sozialen Netzwerken erfolgt häufig grenzüberschreitend. Während es durchaus namhafte soziale Netzwerke gibt, die von Deutschland aus betrieben werden[252], haben jedenfalls Facebook und Google+, als von den Nutzerzahlen bedeutendste soziale Netzwerke[253], ihren Stammsitz im Ausland und zusätzlich weltweite Niederlassungen. Zudem sind die Server, auf welchen die Daten abgespeichert und verarbeitet werden, häufig über die ganze Welt verteilt.[254] Um die Regulierungsmöglichkeiten des deutschen und des europäischen Datenschutzrechts zu beurteilen, muss daher zunächst geklärt werden, inwieweit diese anwendbar sind.

Die datenschutzrechtliche Regulierung sozialer Netzwerke in Deutschland erfolgt aktuell ganz überwiegend durch das BDSG, TMG und TKG. Die Normen beruhen dabei wesentlich auf europarechtlichen Vorgaben der europäischen Datenschutzrechtlinie (DSRL) aus dem Jahr 1995. Zusätzlich existieren die Rahmenrichtlinie über den elektronischen Geschäftsverkehr[255] und die Daatenschutzrichtlinie für elektronische Kommunikation (EK-DSRL)[256] in der Fassung der Richtlinie 2009/136/EG[257], welche zusammen die Richtlinie über den elektronischen Geschäftsverkehr (ECRL)[258] ergänzen. Wie nachfolgend zu zeigen sein wird, entfalten diese aber allenfalls sehr eingeschränkte Wirkung für die Datenschutzregelungen in sozialen Netzwerken.[259]

Nach einem über vier Jahre währenden Verhandlungsprozess ist nunmehr am 14. April 2016 die europäische DS-GVO beschlossen worden, welche das europäische Datenschutzrecht auf eine vollkommen neue Grundlage stellen wird.[260] Die Verhandlungen hierfür wurden stringent,

---

252 Beispielsweise das berufsorientierte soziale Netzwerk Xing und früher die Netzwerke der VZ-Gruppe.

253 Vgl. zu den Nutzerzahlen bereits oben unter B.I.2.

254 Dies kritisiert scharf *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 27.

255 Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste.

256 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

257 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

258 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt.

259 Hierzu unten unter C.I.2.

260 Die DS-GVO wurde am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht (L 199/1) und tritt damit am 25.05.2016 in Kraft; sie gilt ab dem 25.5.2018, vgl. Art. 99 DS-GVO.

aber lange mit verhältnismäßig offenem Ergebnis geführt, so dass erst mit der Einigung auf den Kompromisstext am 15. Dezember 2015, welcher am 17. Dezember 2015 von dem Innen- und Justizausschuss angenommen wurde,[261] ein weitgehend endgültiger Verordnungstext vorlag.[262]

Die DS-GVO wird indes gemäß ihres Art. 91 Abs. 2 erst zwei Jahre nach ihrem Inkrafttreten anwendbar sein, also ab dem 25. Mai 2018. Ihre Regelungen werfen erheblichen Forschungsbedarf auf, beispielsweise in Bezug auf die zahlreichen vagen Formulierungen, insbesondere bei den Erlaubnistatbeständen des Art. 6 DS-GVO[263], dem Umfang der eingeräumten Umsetzungsspielräume der Mitgliedstaaten[264] und Fragen der künftigen Zusammenarbeit der nationalen Datenschutzbehörden gemäß Art. 51 ff. DS-GVO[265].

Die Geltung der DS-GVO bedingt zudem erhebliche Änderungen der nationalen Datenschutzgesetzgebung, indem aufgrund des Anwendungsvorangs des Europarechts der Geltungsbereich des nationalen Datenschutzrechts erheblich beschränkt wird. Dem ist der Gesetzgeber insbesondere durch die Verschiedung des Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU)[266] im Juni 2017 nachgekommen, welches unter anderem eine vollständige Novellierung des BDSG enthält. § 1 Abs. 5 BDSG n.F. stellt dabei

---

261 Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Dok. Nr. 5455/16.

262 Auf den ersten Entwurf der europäischen Kommission vom 25. Januar 2012 (Vorschlag für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.1.2012, KOM (2012) 11 endgültig) wurde vom europäischen Parlament eine umfangreiche Überarbeitung des Entwurfes angefertigt, in dessen Prozess über dreitausend Änderungsvorschläge bearbeitet wurden. Das Ergebnis wurde am 21. Oktober 2013 von dem zuständigen Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments angenommen (im Folgenden LIBE-Entwurf). Die Bestätigung durch das Plenum erfolgte am 12. März 2014 mit einer überwältigenden Mehrheit von 621 befürwortenden Stimmen, bei 10 Nein-Stimmen und 22 Enthaltungen (Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, P7_TA-PROV(2014)0212). Am 15. Juni 2015 konnten sich sodann auch der Rat der Innen- und Justizminister auf eine gemeinsame Position einigen und einen erneut modifizierten dritten Entwurf präsentieren (Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr – Vorbereitung einer allgemeinen Ausrichtung, Dok. Nr. 9565/15). Die am 24. Juni 2015 begonnenen Trilogverhandlungen gemäß Art. 294 AEUV zwischen dem Parlament, dem Rat und der Kommission führten sodann zur Einigung und dem zuvor genannten Kompromisstext. Vgl. für Analysen des Gesetzgebungsprozess auch statt vieler *Roßnagel/Kroschwald*, ZD 2014, 495 (495 ff.); *Roßnagel/Nebel/Richter*, ZD 2015, 455 (455 ff.).

263 Kritisch hierzu *Nebel/Richter*, ZD 2012, 407 (408 ff.); *Sydow/Kring*, ZD 2014, 271 (272 f.); *Roßnagel/Kroschwald*, ZD 2014, 495 (497); *Roßnagel/Nebel/Richter*, ZD 2015, 455 (457).

264 Hierzu bereits *Koós*, ZD 2014, 9 (13 f.); vgl. auch *Klar*, DÖV 2013, 103 (111 f.).

265 Vgl. *Koós*, ZD 2014, 9 (14); *Dieterich*, ZD 2016, 260 (264 f.).

266 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, BGBl. I 2017, S. 2097 ff.

deklaratorisch den Anwendungsvorrang der DS-GVO fest, soweit deren Anwendungsbereich reicht.

Wie sich im Verlaufe dieser Arbeit zeigen wird, werden sich auch nach Einführung der DS-GVO viele der grundlegenden und sehr praxisrelevanten Fragen der bisherigen Rechtslage weiterhin stellen, da sie keiner legislativen Lösung zugeführt wurden.[267] Dies betrifft insbesondere die schwerpunktmäßig in dieser Arbeit untersuchten Probleme der datenschutzrechtlichen Verantwortlichkeit in mehrseitigen Rechtsbeziehungen und der Einwilligung in die Datenverarbeitung durch die Nutzer.

Um den Umfang dieser Arbeit zu begrenzen, ist das Erkenntnisinteresse auf die in der bisherigen Rechtslage bereits angelegten Probleme beschränkt. Es wird untersucht, wie die legislativen Antworten bisher und zukünftig aussehen und inwieweit sie einer Modernisierung bedurften. Während der Ausgangspunkt der Betrachtung dabei die Regelungen der DS-GVO sind, liegt der Schwerpunkt dennoch auf der Betrachtung des bisherigen nationalen Rechts. Dies ist einerseits in der langen Übergangsfrist der DS-GVO begründet und andererseits der hohen Praxisrelevanz der aktuellen Regelungen, die sich nicht zuletzt in mehreren anhängigen bzw. erst kürzlich entschiedenen Vorabentscheidungsverfahren gemäß Art. 267 AEUV beim EuGH äußert.[268] Zudem bietet es sich angesichts der häufigen Vagheit der neuen Regelungen an, zumindest zur Bildung von dogmatischen Fallgruppen auf das bisherige, deutlich detailliere und bereichsspezifischere Datenschutzrecht zurückzugreifen.[269]

Im Folgenden soll zunächst der zukünftige Anwendungsbereich der DS-GVO betrachtet und die fortdauernde Relevanz der bisherigen kollisionsrechtlichen Fragestellungen erörtert werden (I.). Anschließend soll die kollisionsrechtliche Anwendbarkeit der bisherigen Regelungsregime untersucht werden (II.). Hierbei liegt der Fokus auf der Frage, nach welchen Kollisionsnormen sich das anwendbare Recht nach gegenwärtiger Rechtslage in Deutschland bestimmt und wie diese auszulegen sind. In einem zweiten Schritt soll der Umfang der materiellen Anwendbarkeit der aktuell noch geltenden nationalen Regelungen im BDSG, TMG und TKG auf soziale Netzwerke näher beleuchtet werden (III.).

---

267 Vgl. auch *Martini/Fritsche*, NVwZ-Extra (21) 2015, 1 (16); *Roßnagel/Kroschwald*, ZD 2014, 495 (499 f.); *Roßnagel/Nebel/Richter*, ZD 2015, 455 (456 ff.); *Cebulla*, ZD 2015, 507 (511 f.); *Sydow/Kring*, ZD 2014, 271 (272 f., 275).

268 Vgl. u.a. BVerwG, ZD 2016, 393 (393 ff.); BGH, ZD 2015, 80 (80 ff.).

269 Hierzu ausführlich unten unter C.I.2 und D.I.3.

I. Anwendungsbereich der DS-GVO

1. Kollisionsrechtliche Anwendbarkeit gemäß Art. 3 DS-GVO

Die DS-GVO normiert als innereuropäisches Kollisionsrecht in Art. 3 Abs. 1 DS-GVO dem bisherigen Art. 4 lit. a) DSRL entsprechend ein Sitzprinzip: Die kollisionsrechtliche Anwendbarkeit der Verordnung folgt aus der Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit einer verantwortlichen Stelle oder eines Auftragsverarbeiters mit Sitz in der Union. Dabei kommt es nicht darauf an, ob die konkrete Datenverarbeitung auf dem Gebiet der Union erfolgt. Die innereuropäische Datenverarbeitung wird damit im Rahmen der materiellen Anwendbarkeit der Verordnung aufgrund ihrer unmittelbaren Anwendbarkeit einem einheitlichen Regelungsstandard unterworfen.[270]

Für nicht in der Union niedergelassene Datenverarbeiter statuiert Art. 3 Abs. 2 DS-GVO eine extraterritoriale Wirkung des europäischen Datenschutzrechts, indem er explizit ein Marktortprinzip festsetzt.[271] Wie unten noch zu zeigen sein wird, ergab sich ein entsprechendes Marktortprinzip in weiten Teilen zwar bereits faktisch aus der funktionell-wirtschaftlichen Auslegung des Art. 4 lit. a) DSRL durch den EuGH.[272] Mit der ausdrücklichen Normierung wird dieser erhöhte Schutz europäischer Bürger weiter verstärkt und rechtssicherer gemacht: Nach Art. 3 Abs. 2 DS-GVO soll die DS-GVO immer dann anwendbar sein, wenn die Datenverarbeitung dem Angebot von Waren oder Dienstleistungen an Unionsbürger dient oder der Beobachtung ihres Verhaltens innerhalb des Territoriums der Union.

Im ursprünglichen Kommisionsentwurf blieb zunächst unklar, wann ein „Anbieten" genau vorliegt und inwieweit ein späterer Vertragsschluss bzw. eine Entgeltlichkeit des angebotenen für dieses Merkmal von Bedeutung ist.[273] Zur Klärung wurde überzeugend vorgeschlagen, das „Anbieten" vergleichbar mit dem „Ausrichten" in Art. 6 Abs. 1 Rom-I VO und Art. 15 Abs. 1 lit. c) EuGVVO auszulegen.[274] Auf das Erfordernis der Kausalität für einen späteren Vertrag sei hierbei zu verzichten, da eine entsprechende Voraussetzung nicht in Art. 3 Abs. 2 DS-GVO

---

270 *Klar*, DÖV 2013, 103 (111); *Nebel/Richter*, ZD 2012, 407 (407 ff.); *Kühling/Martini*, EuZW 2016, 448 (448 ff.) weisen allerdings zurecht auf zahlreiche Öffnungsklauseln für mitgliedstaatliche Regelungen hin, welche die DS-GVO faktisch zu einem „Hybrid aus Verordnung und Richtlinie" mache; ausführlich zum Anwendungsbereich auch *Barlag*, in: Roßnagel (Hrsg.), Europäische DS-GVO, § 3 Rn. 1 ff.

271 *Kühling/Martini*, EuZW 2016, 448 (450); *Roßnagel/Kroschwald*, ZD 2014, 495 (497); *Spindler*, GRUR-Beilage 2014, 101 (107 f.); *Nolte*, NJW 2014, 2238 (2240); *Klar*, DÖV 2013, 103 (111); *Spiecker gen. Döhmann*, K&R 2012, 717 (719).

272 Hierzu unten unter C.II.4.b)bb); vgl. auch *Beyvers/Herbrich*, ZD 2014, 558 (562); kritisch: *Pauly/Ritzer/Geppert*, ZD 2013, 423 (424).

273 *Piltz*, K&R 2013, 292 (297); *Klar*, ZD 2013, 109 (113).

274 *Piltz*, K&R 2013, 292 (297).

statuiert sei und es zudem widersinnig wäre, die Anwendbarkeit des Datenschutzrechts im Vorfeld von Vertragsverhandlungen davon abhängig zu machen, dass später ein Vertrag abgeschlossen werde. Die Regelung fände folglich auch auf solche Anbieter Anwendung, die Websites bereithalten, aber nicht direkt die Möglichkeit eines Vertragsschlusses bieten.[275] Eine dieser Auslegung entsprechende Klarstellung wurde durch den *LIBE*-Entwurf eingeführt, welcher den Art. 3 Abs. 2 lit. a) DS-GVO um die Formulierung ergänzte, dass er „unabhängig davon, ob von der betroffenen Person eine Zahlung zu leisten ist", gelte.[276] Diese Formulierung wurde nunmehr auch in der endgültigen Fassung übernommen.

Ein Angebot von sozialen Netzwerken an Bürger innerhalb der EU unterfällt daher in jedem Fall dem kollisionsrechtlichen Anwendungsbereich der DS-GVO, unabhängig davon, in welchem Land der Anbieter seinen Sitz hat, welche Form von Vertrag über die Nutzung abgeschlossen wird und ob die preisgegebenen Daten als „Entgelt" anzusehen sind.[277] Es steht zu hoffen, dass diese weite Anwendbarkeit des europäischen Datenschutzrechts eine positive Wirkung auf den Datenschutzstandard weltweit haben wird. Denn während natürlich die Regulierungshoheit der anderen Staaten unangetastet bleibt, führt die Marktmacht der EU doch dazu, dass sich die meisten globalen Internetangebote zwingend mit den europäischen Standards auseinandersetzen müssen.[278] Sie werden entsprechend eine Entscheidung treffen müssen, ob sie ihr gesamtes Angebot auf den strengsten Datenschutzstandard ausrichten oder aber je nach Marktort unterschiedliche Standards anwenden und entsprechende parallele Strukturen in ihrem Angebot aufbauen. Maßgeblich wird hierbei vor allem die ökonomische Abwägung sein, ob die mit einem Verzicht auf parallele Strukturen gesparten Kosten die entgangenen Gewinne einer umfangreicheren Datenverarbeitung in anderen Märkten überwiegen.[279]

2. Materiellrechtlicher Anwendungsbereich und Anwendungsvorrang

Materiell ersetzt die DS-GVO gemäß Art. 94 Abs. 1 DS-GVO vollständig die DSRL 95/46/EG, welche aufgehoben wird. Als unmittelbar anwendbares Recht mit einem Umsetzungsverbot für die Mitgliedstaaten in ihrem Anwendungsbereich gemäß Art. 288 Abs. 2 AEUV werden daher

---

275 *Piltz*, K&R 2013, 292 (297); vgl. auch *Klar*, ZD 2013, 109 (113); *Simitis*, in: Simitis, BDSG, § 1 Rn. 241.
276 *Roßnagel/Kroschwald*, ZD 2014, 495 (497).
277 Auf einem anderen Blatt steht freilich, inwieweit die EU diese extraterritoriale Wirkung auch durchsetzen wird, insbesondere angesichts weitreichender Datenverarbeitungswünsche durch US-amerikanische Behörden, vgl. bereits *Spiecker gen. Döhmann*, K&R 2012, 717 (719); zweifelnd auch *Koós/Englisch*, ZD 2014, 276 (278).
278 *Klar*, DÖV 2013, 103 (111); *Ders*., ZD 2013, 109 (114); vgl. auch *Herrmann*, ZD 2014, 439 (440).
279 Vgl. *Schantz*, NJW 2016, 1841 (1842) m.w.N.

auch große Teile des aktuell geltenden nationalen Datenschutzrechts unanwendbar werden.[280] Hierauf hat der nationale Gesetzgeber inzwischen durch die Verabschiedung des DSAnpUG-EU reagiert, welches gemäß seinem Artikel 8 Abs. 1 zum 25. Mai 2018 in Kraft tritt, also mit Inkrafttreten der DS-GVO.

Speziell die Datenverarbeitung durch Private in sozialen Netzwerken wird einer umfassenden Regelung durch die DS-GVO unterliegen – mit der Folge, dass die Regelungen des BDSG n.F. (Art. 1 DSAnpUG-EU) verdrängt werden – soweit den Mitgliedstaaten nicht spezielle Regelungsbefugnisse eingeräumt werden.

Ein möglicher solcher Spielraum könnte in der Regelung des Art. 85 DS-GVO liegen, welcher die Mitgliedstaaten ermächtigt, eigene Gesetze zum Ausgleich der informationellen Selbstbestimmung und der Meinungs- und Informationsfreiheit zu erlassen, da soziale Netzwerke von ihren Nutzern sehr effektiv zur Verbreitung von Meinungen eingesetzt werden können.[281] Hierbei darf allerdings nicht übersehen werden, dass jedenfalls bisher soziale Netzwerke nicht als journalistisch-redaktionelle Inhalte i.S.v. § 41 BDSG eingestuft wurden[282] und es daher fraglich ist, ob ihre Regulierung unter Art. 85 DS-GVO fallen würde. Ferner kann eine eventuelle Verarbeitung von personenbezogenen Daten durch öffentliche Stellen zu Zwecken des Gemeinwohls nach Art. 6 Abs. 1 lit. e) DS-GVO gemäß Art. 6 Abs. 2 DS-GVO durch mitgliedstaatliche Regelungen spezifiziert werden. Eine weitere mögliche Öffnung könnte sich aus Art. 6 Abs. 1 lit. c) i.V.m. Art. 6 Abs. 2 DS-GVO ergeben, soweit eine Datenverarbeitung zur Erfüllung von Verpflichtungen erforderlich ist, denen der Verantwortliche nach mitgliedstaatlichem Recht unterliegt.[283]

Das DSAnpUG-EU nutzt zudem bereits den in Art. 9 Abs. 4 DS_GVO normierten Spielraum und stellt insbesondere in den §§ 22 ff. BDSG n.F. zusätzliche Bedingungen für die Verarbeitung besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DS-GVO auf. Soweit derzeit ersichtlich, werden diese Regelungen für die Datenverarbeitung durch

---

280 *Nebel/Richter*, ZD 2012, 407 (408); *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 129; ausführlich: *Keppeler*, MMR 2015, 779 (780 ff.); *Schantz*, NJW 2016, 1841 (1841 ff.); vgl. allgemein zur unmittelbaren Anwendbarkeit von Verordnungen *Haratsch/Koenig/Pechstein*, Europarecht, Rn. 382 f.; vgl. allerdings für einen instruktiven Überblick der den Mitgliedstaaten überlassenen Regelungsbereiche *Dammann*, ZD 2016, 307 (310 f.); *Schaller u.a.*, in: Roßnagel (Hrsg.), Europäische DS-GVO, § 4 Rn. 17 ff.

281 So auch *Martini*, VerwArch (107) 2016, 307 (350), der allerdings zugleich darauf hinweist dass es sich nicht um eine Öffnungsklausel im engeren Sinne handelt, sondern Art. 85 Abs. 1 DS-GVO i.V.m. Erwägungsgrund 153 S. 1 DS-GVO explizit nur Ausnahmen für spezifische, insbesondere journalistische Zwecke zulässt.; ausführlich auch *Hoidn*, in: Roßnagel (Hrsg.), Europäische DS-GVO, § 4 Rn. 160 ff.

282 Hierzu unten unter D.I.3.a)cc).

283 Vgl. hierzu bereits *Koós*, ZD 2014, 9 (13 f.); *Martini*, VerwArch (107) 2016, 307 (349); ausführlich zu Öffnungsklauseln in der DS-GVO auch *Kühling/Martini*, EuZW 2016, 448 (448 ff.).

Private in sozialen Netzwerken aber allenfalls eine anekdotische Bedeutung erlangen, da sie weitestgehend andere Sachverhalte betreffen.

Erwägungsgrund 10 DS-GVO weist zudem ausdrücklich auf bestehende sektorspezifische Datenschutzgesetze der Mitgliedstaaten in Umsetzung der früheren DSRL 95/46/EG hin und deutet an, dass insoweit Umsetzungsspielräume verbleiben können:

> „In Verbindung mit den allgemeinen und horizontalen Rechtsvorschriften über den Datenschutz zur Umsetzung der Richtlinie 95/46/EG gibt es in den Mitgliedstaaten mehrere sektorspezifische Rechtsvorschriften in Bereichen, die spezifischere Bestimmungen erfordern. Diese Verordnung bietet den Mitgliedstaaten darüber hinaus einen gewissen Spielraum für die Spezifizierung ihrer Vorschriften, auch für die Verarbeitung besonderer Kategorien von personenbezogenen Daten (im Folgenden „sensible Daten"). Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist."

Für die deutsche Rechtslage könnte dies vor allem für die telemedienrechtlichen Datenschutzvorschriften der §§ 11 ff. TMG von Bedeutung sein. Diese Regelungen, die auf das im Rahmen des Informations- und Kommunikationsdienstegesetzes (IuKDG) verabschiedete Teledienstedatenschutzgesetz (TDDSG)[284] aus dem Jahr 1997 zurückgehen, wurden als bereichsspezifische Konkretisierungen des Datenschutzrechts erlassen.[285] Während weder in der Gesetzesbegründung zum IuKDG noch zum TMG ausdrücklich auf die DSRL 95/46/EG Bezug genommen wurde, handelt es sich im Ergebnis um zulässige, bereichsspezifische Konkretisierungen der Richtlinie.[286]

Die Regelungen der §§ 11 ff. TMG beruhen dagegen nicht auf der EK-DSRL 2002/58/EG.[287] Dies folgt nicht zuletzt aus Art. 3 Abs. 1 EK-DSRL, der den Anwendungsbereich der Richtlinie auf elektronische Kommunikationsdienste beschränkt, welche wiederum in Art. 2 lit.c) der Rahmenrichtlinie über den elektronischen Geschäftsverkehr legaldefiniert werden: Umfasst

---

284 BT-Drs. 13/7385, S. 6 ff.; BGBl. I 1997, S. 1870 f.

285 *Engel-Flechsig*, Beck'scher IuKDG Kommentar, Einf TDDSG, Rn. 29; *Schulz*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, § 1 TDDSG, Rn. 21, § 5 TDDSG, Rn. 20, § 6 TDDSG Rn. 16; BT-Drs. 13/7385, S. 21 ff.

286 *Engel-Flechsig*, Beck'scher IuKDG Kommentar, Einf TDDSG, Rn. 30; *Schulz*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, § 1 TDDSG, Rn. 21; vgl. auch *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 129.

287 *Schmitz*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 16.2, Rn. 36; *Keppeler*, MMR 2015, 779 (781); *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 129; *Gola/Schulz*, ZD 2013, 475 (477); *Nebel/Richter*, ZD 2012, 407 (408); *Geminn/Richter*, in: Roßnagel (Hrsg.), Europäische DS-GVO, § 4 Rn. 267.

sind demnach nur solche Dienste, die in der Regel gegen Entgelt erbracht werden und ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetzwerke bestehen. Erwägungsgrund 10 der Rahmenrichtlinie stellt hierbei klar, dass Dienste, die in der „Bereitstellung von Internet gestützten Inhalten bestehen", keine elektronischen Kommunikationsdienste darstellen und entsprechend auch nicht von der der Richtlinie erfasst sind. [288] Die EK-DSRL und auf ihr beruhende Regelungen im TMG sind daher für soziale Netzwerke, die jedenfalls in ihrer Gesamtheit keine elektronischen Kommunikationsdienste darstellen[289], nur indirekt von Bedeutung, beispielsweise für das rechtmäßige Setzen von Cookies zur Ermöglichung zielgerichteter, verhaltensbasierter Werbung.[290] Die Einschränkung des Anwendungsbereichs gemäß Art. 95 DS-GVO im Verhältnis zu Pflichten, die durch die der EK-DSRL 2002/58/EG aufgestellt werden, wirkt sich für soziale Netzwerke entsprechend nur sehr begrenzt aus. Vergleichbares gilt für die ePrivacyVO, welche derzeit auf europäischer Ebene verhandelt wird und die EK-DSRL 2002/58/EG ablösen soll.[291] Der im Januar 2017 verabschiedete Kommissionsentwurf[292] beschränkt den Anwendungsbereich der ePrivacyVO – wie bisher die EK-DSRL – vornehmlich auf die Regulierung elektronischer Kommunikationsdienste (Art. 2 ePrivacyVO-E). Zudem wird klargestellt, dass es sich um eine bereichsspezifische Ergänzung und Präzisierung der Regelungen der DS-GVO handele, Art. 1 Abs. 3 ePrivacyVO-E.

Insoweit ist davon auszugehen, dass die datenschutzrechtlichen Regelungen der §§ 11 ff. TMG grundsätzlich dem zukünftigen Anwendungsbereich der DS-GVO unterfallen und insoweit verdrängt werden.[293]

Wie unten unter D.I.3. zu zeigen sein wird, wird hierdurch allerdings eine erhebliche Rechtsunsicherheit geschaffen, da die DS-GVO in Abkehr von einem bereichsspezifischen Ansatz einen radikal technologieneutralen Ansatz verfolgt und daher in Art. 6 DS-GVO –

---

288 *Nebel/Richter*, ZD 2012, 407 (408); *Gola/Schulz*, ZD 2013, 475 (477); vgl. mit Verweis auf Abgrenzungsprobleme auch *Schulz*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, § 1 TDDSG, Rn. 22.

289 Hierzu ausführlich unten unter C.III.1.

290 Hierzu ausführlich unten unter D.I.3.c)aa)i).

291 Vgl. instruktiv zur ePrivacyVO *Schleipfer*, ZD 2017, 460 (463 ff.).

292 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), vom 10. Januar 2017, COM(2017) 10 final, Dok. Nr. 2017/0003 (COD).

293 Sehr ausführlich, mit differenzierter Analyse der einzelnen Normen: *Geminn/Richter*, in: Roßnagel (Hrsg.), Europäische DS-GVO, § 4 Rn. 267 ff.; vgl. auch *Schmitz*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 16.2, Rn. 36; *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 129; *Nebel/Richter*, ZD 2012, 407 (408); *Roßnagel/Richter/Nebel*, ZD 2013, 103 (103 f.).

nahezu wortgleich zum bisherigen vollharmonisierenden, aber durch mitgliedstaatliche Vorschriften dennoch konkretisierbaren Art. 7 DSRL – nur sehr abstrakte, undifferenzierte Erlaubnistatbestände für die Datenverarbeitung enthält.[294] Jedenfalls zur Schaffung von Fallgruppen bietet es sich daher an, auch weiterhin auf die Differenzierung insbesondere zwischen Bestands- und Nutzungsdaten der §§ 14, 15 TMG zurückzugreifen. Insbesondere die durch Art. 6 Abs. 1 lit. f) DS-GVO vorgegebene Interessenabwägung, aber auch die für eine Vertragsdurchführung notwendigen Daten nach Art. 6 Abs. 1 lit. b) DS-GVO lassen sich so dogmatisch vorstrukturieren.[295]

Ob derartige Regelungen darüber hinaus nach Erwägungsgrund 10 DS-GVO zulässige, mitgliedstaatliche, bereichsspezifische Konkretisierungen darstellen und daher auch formal von dem Anwendungsvorrang ausgenommen sind, wird letztendlich abstrakt im Rahmen eines Vorabentscheidungsverfahren gemäß Art. 267 AEUV durch den EuGH zu entscheiden sein. An dieser Stelle kann nur festgehalten werden, dass nach Wortlaut und Telos des Erwägungsgrundes eine solche Auslegung vertretbar erscheint und angesichts des erheblichen Gewinns an Rechtssicherheit sogar sehr zu begrüßen wäre. Systematisch ließe sich indes dagegen einwenden, dass das Kapitel 9 der DS-GVO explizit Bereiche aufzählt, in denen den Mitgliedstaaten eigene Regelungsbefugnisse zugestanden werden und das Telemedienrecht hiervon – außerhalb des möglicherweise von Art. 85 DS-GVO eröffneten Regelungsspielraums – nicht umfasst ist. Ob das Kapitel 9 insoweit eine abschließende Konkretisierung des Erwägungsgrundes 10 darstellt oder nur deutlich über eine gesetzgeberische Standardisierung der Interessenabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO hinausgehende Regelungsbefugnisse statuiert, kann hier nicht abschließend geklärt werden.[296]

3. Fortdauernde Bedeutung aktueller kollisionsrechtlicher Fragestellungen

Die DS-GVO beseitigt viele der aktuell existierenden Abgrenzungsprobleme sowohl auf kollisionsrechtlicher als auch materieller nationaler Ebene, indem ein einheitlicher Rechtsrahmen für die Datenverarbeitung geschaffen wird. Die Frage nach der konkret verantwortlichen Stelle verliert ihre kollisionsrechtliche Bedeutung, da innerhalb der EU –

---

294 Vgl. auch *Roßnagel*, in: Ders. (Hrsg.), Europäische DS-GVO, § 1 Rn. 29 ff.; *Schleipfer*, ZD 2017, 460 (461 ff.).

295 Hierzu ausführlich unten unter D.I.3; in diese Richtung auch *Nebel*, in: Roßnagel (Hrsg.), Europäische DS-GVO, § 3 Rn. 109.

296 Weitergehende Regelungsbefugnisse ablehnend: *Keppeler*, MMR 2015, 779 (781).

anstelle von mitgliedstaatlichen Regelungen – der identische Datenschutzstandard der DS-GVO gelten wird.[297]

Die Bestimmung der konkret verantwortlichen Stelle könnte allerdings im Zusammenhang mit der zuständigen Aufsichtsbehörde von Bedeutung bleiben. Art. 55 DS-GVO erklärt nationale Datenschutzbehörden für zuständig, im Territorium ihrer jeweiligen Mitgliedstaaten über die Umsetzung der DS-GVO zu wachen. Mögliche Konflikte werden weitgehend durch Art. 56 Abs. 1 DS-GVO entschärft, welcher im Falle von mehreren Niederlassungen eines Datenverarbeiters die Aufsichtsbehörde der Hauptniederlassung innerhalb der EU für federführend erklärt. Die Art. 60 ff. DS-GVO konkretisieren zudem das Verhältnis und die Pflichten zur Zusammenarbeit der unterschiedlichen hiernach zuständigen Aufsichtsbehörden.[298] Welche nationale Aufsichtsbehörde dabei innerhalb Deutschlands konkret zuständig ist, wird sich nach den Regelungen der §§ 18 f., 40 BDSG n.F. gemäß Art. 1 DPAnpUG-EU richten.

Von der zukünftigen Forschung und Rechtspraxis wird indes zu klären sein, unter welchen Umständen von einem Vorliegen der Ausnahme des Art. 56 Abs. 2 DS-GVO auszugehen ist, wonach abweichend von Art. 56 Abs. 1 DS-GVO eine nationale Aufsichtsbehörde zuständig sein soll, „wenn der Gegenstand [einer Beschwerde] nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres Mitgliedstaats erheblich beeinträchtigt“. Speziell die nationalen Niederlassungen Facebooks, wie beispielsweise die *Facebook Germany GmbH*, könnten hier Anlass für komplexe Zuständigkeitsauseinandersetzungen der Aufsichtsbehörden bieten, wenn man die Ausführungen des EuGH im Urteil zu *Google Spain*[299] zur Frage der verantwortlichen Stelle berücksichtigt. Zwar besteht grundsätzlich kein Zweifel daran, dass es sich bei der *Facebook Ireland Ltd.* um die Hauptniederlassung Facebooks im europäischen Raum handelt, auch wenn ihre rechtliche Eigenständigkeit gegenüber der Muttergesellschaft *Facebook Inc.* in den USA

---

297 Die bloße Vereinheitlichung des Gesetzestexts vermag freilich nicht zu überdecken, dass aktuell noch sehr unterschiedliche Wertevorstellungen in den Mitgliedstaaten der EU bei der Abwägung von Freiheit, Sicherheit und Persönlichkeitsrechten existieren. Diese können zu voneinander abweichenden Interpretationen des Verordnungstexts in der Praxis führen und damit zahlreiche Vorabentscheidungsverfahren beim EuGH erforderlich machen, bevor tatsächlich Rechtssicherheit und eine einheitliche Rechtsanwendung sichergestellt sind, so bereits *Klar*, DÖV 2013, 103 (111 f.); die sehr weiten Erlaubnistatbestände des Art. 6 DS-GVO, insb. des lit. f) werden diese Problematik weiter befördern, vgl. *Roßnagel/Nebel/Richter*, ZD 2015, 455 (457); kiritisch zum einheitlichen Vollzug unter Verweis auf frühere Schwierigkeiten etwa bei der Durchsetzung von vereinheitlichten Gerichtsstandsklauseln *Dieterich*, ZD 2016, 260 (261 ff.).

298 Vgl. instruktiv *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 132; *Nguyen*, ZD 2015, 265 (266 ff.).

299 EuGH, *Google Spain*, Rs. C-131/12 = JZ 2014, 1009 ff.; hierzu ausführlich unten unter C.II.4.b)bb).

zutreffend in Frage gestellt werden kann.[300] Allerdings sind es die nationalen Niederlassungen wie die *Facebook Germany GmbH*, die die Nutzerdaten mit der den Nutzern anzuzeigenden Werbung verknüpfen und hierfür entsprechende Werbeakquise betreiben; erst sie begründen überhaupt die Rentabilität des sozialen Netzwerks Facebook.[301] Wie nachfolgend zu zeigen sein wird, führt diese Verknüpfung dazu, dass die *Facebook Germany GmbH* und vergleichbare nationale Niederlassungen unter Zugrundelegung des gebotenen wirtschaftlich-funktionellen Verantwortlichkeitsbegriffs als voll verantwortliche Stellen der Datenverarbeitung Facebooks im Sinne der aktuellen kollisionsrechtlichen Regelungen anzusehen sind.[302]

Angesichts dieser Zusammenhänge erscheint es jedenfalls nicht ausgeschlossen, gemäß Art. 56 Abs. 2 DS-GVO eine Zuständigkeit der deutschen Datenschutzbehörden für die Tätigkeit Facebooks in Deutschland anzunehmen.[303] Auch in diesem Fall bestünde zwar eine Verpflichtung, die irische Datenschutzbehörde gemäß Art. 56 Abs. 3 DS-GVO über Beschwerden gegen Facebook zu informieren; diese hätte daraufhin innerhalb einer Frist von drei Wochen die Gelegenheit, die Hoheit über das Verfahren gemäß Art. 60 DS-GVO als federführende Aufsichtsbehörde an sich zu ziehen. Dennoch käme den nationalen Aufsichtsbehörden jedenfalls ein besonderes Initiativrecht zu und die Möglichkeit der Federführung, soweit die irische Datenschutzbehörde keine Übernahme der Federführung begehrt.

Ob diese Auslegung in der Praxis Bestand haben wird, kann in letzter Konsequenz nur durch den EuGH entschieden werden. Sie zeigt aber, dass eine Beschäftigung mit den Fragen der verantwortlichen Stelle und den Konsequenzen aus dem *Google*-Urteil des EuGH nicht nur für die bisherige kollisionsrechtliche Lage erforderlich ist, sondern auch für die Auslegung der DS-GVO erhebliche Bedeutung hat. Die Beschäftigung mit diesen Fragen erweist sich daher nach wie vor als geboten.

Zusammenfassend lässt sich feststellen, dass die DS-GVO die ganz überwiegende Mehrheit der bisherigen kollisionsrechtlichen Fragen löst, indem sie die Anwendbarkeit eines einheitlichen europäischen Datenschutzrechts nach einem kombinierten Sitz- und Marktortprinzip anordnet. Dennoch bleibt es aus all den aufgezeigten Gründen relevant, auch die noch unbeantwortet

300 Hierzu unten unter C.II.4.a).
301 Hierzu unten unter C.II.4.b)cc).
302 Hierzu unten unter C.II.4.b)cc).
303 Auf die Möglichkeit der Zuständigkeit verschiedener Aufsichtsbehörden, entgegen des von der DS-GVO angestrebten One-Stop-Shop-Prinzips, weisen abstrakt auch bereits hin: *Nguyen*, ZD 2015, 265 (267); *Gierschmann*, ZD 2016, 51 (51 f.).

gebliebenen kollisionsrechtlichen Fragen der bisherigen Rechtslage zu klären. Dem soll nun im Folgenden nachgegangen werden.

II. Kollisionsrechtliche Anwendbarkeit des BDSG, TMG und TKG

Wie praxisrelevant und zugleich noch ungeklärt die Frage nach dem anwendbaren nationalen Datenschutzrecht in der bisherigen Rechtslage ist, zeigt sich nicht zuletzt an mehreren aktuellen Gerichtsverfahren, in denen streitig war und teilweise gegensätzlich beantwortet wurde, ob Facebook bei der Verarbeitung personenbezogener Daten in Deutschland deutschem Datenschutzrecht unterliegt.[304] In diesem Zusammenhang ist insbesondere die Entscheidung des EuGH zu *Google Spain* vom Mai 2014[305] näher zu analysieren. Die kollisionsrechtliche Behandlung Facebooks ist ferner Gegenstand eines Revisionsverfahrens am Bundesverwaltungsgericht und wurde mit Beschluss vom 25. Februar 2016 dem EuGH zur Vorabentscheidung nach Art. 267 AEUV vorgelegt.[306]

1. Maßgebliche Kollisionsnormen

Die in § 3 Abs. 1 und 2 TMG statuierten Kollisionsregeln gelten gemäß § 3 Abs. 3 Nr. 4 TMG nicht für das Recht zum Schutz personenbezogener Daten. In Ermangelung einer spezialgesetzlichen Regelung im TMG und TKG regelt daher § 1 Abs. 5 BDSG die kollisionsrechtliche Anwendbarkeit des deutschen Datenschutzrechts.[307] Im Ergebnis[308] führt die Regelung des § 1 Abs. 5 BDSG dazu, dass in jedem Fall die durch die europäische DSRL vorgegebenen (Mindest-)Standards einzuhalten sind.

Gegen die Maßgeblichkeit des § 1 Abs. 5 BDSG wird von einigen Autoren vorgebracht, dass dieser den Art. 4 DSRL nur unzureichend umsetze und daher zur Bestimmung des anwendbaren Rechts – angesichts einer postulierten umfassenden Harmonisierungswirkung der Richtlinie

---

304 Eine Anwendbarkeit bejaht beispielsweise KG Berlin, ZD 2014, 412 (414); dagegen verneint von OVG Schleswig, ZD 2013, 364 (366); VG Schleswig, ZD 2013, 245 (245 f.); VG Hamburg, ZD 2016, 243 (244 ff.).

305 EuGH, *Google Spain*, Rs. C-131/12, Rn. 52 = JZ 2014, 1009 ff.

306 BVerwG, ZD 2016, 393 (393 ff.).

307 *Kremer*, RDV 2014, 73 (75); *Karg*, ZD 2013, 371 (372); *Plitz*, Soziale Netzwerke im Internet, S. 71; *Piltz*, K&R 2012, 640 (641); *Polenz*, VuR 2012, 207 (208); *Weller/Nordmeier*, in: Spindler/Schuster, Art. 9 Rom I-VO, Rn. 14; *Dammann*, in: Simitis, BDSG, § 1 Rn. 213; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 53; *Jotzo*, MMR 2009, 232 (234); BGH, NJW 2012, 2197 (2198); VG Hamburg, ZD 2016, 243 (244); a.A. *Voigt*, K&R 2014, 325, 327, der für eine direkte Anwendbarkeit des Art. 4 DSRL plädiert.

308 Zur ausführlicheren Betrachtung insbesondere der zwingenden Anwendbarkeit anstelle einer individuellen Rechtswahl vgl. sogleich unten C.II.3.

und einer hinreichenden Bestimmtheit des Art. 4 DSRL – direkt auf Art. 4 DSRL zurückzugreifen sei.[309]

Dem ist nicht zu folgen. Vielmehr ist § 1 Abs. 5 BDSG richtlinienkonform auszulegen, soweit er hinter den Vorgaben der Richtlinie zurückbleibt.[310] Die unmittelbare Anwendbarkeit einer Richtlinie dient dazu, die Durchsetzung von Individualrechten gegen den Staat zu ermöglichen, sofern diese in der Richtlinie hinreichend bestimmt und unbedingt festgeschrieben wurden und die Umsetzungsfrist abgelaufen ist, im nationalen Recht aber dennoch keine entsprechenden Rechtsgrundlagen geschaffen wurden.[311] Eine unmittelbare Drittwirkung gegenüber anderen Privaten wird ganz herrschend abgelehnt, eine mittelbare Drittwirkung wird nur unter engen Voraussetzungen akzeptiert.[312] Bei der Frage nach der richtlinienkonformen Umsetzung in § 1 Abs. 5 BDSG handelt es sich um eine Frage des Kollisionsrechts und nicht um eine materieller Anspruchsbegründung. Damit geht es schon ganz grundsätzlich nicht um die Durchsetzung der von in Art. 4 DSRL garantierten Individualrechte. Es handelt sich um eine andere Konstellation als bei der unmittelbaren Anwendbarkeit von Richtlinien. Freilich ist das Kollisionsrecht indirekt für materielle Ansprüche relevant, wenn infolge dessen ein mitgliedstaatliches Recht Anwendung findet, das hinreichend bestimmte Individualrechte nicht fristgemäß umgesetzt hat. Auch in diesem Fall kann aber allenfalls hinsichtlich des konkreten Anspruchs eine unmittelbare Anwendbarkeit der jeweiligen materiellen Bestimmung der Richtlinie in Betracht kommen, nicht aber eine unmittelbare Anwendung der Kollisionsnorm. Entsprechend kann nicht auf die Grundsätze der unmittelbaren Anwendbarkeit zurückgegriffen werden, insbesondere wenn auch das „mildere“ Mittel der richtlinienkonformen Auslegung verfügbar ist. § 1 Abs. 5 BDSG ist einer solchen Auslegung zugänglich und damit die richtige Kollisionsnorm.[313]

---

309 *Kremer*, RDV 2014, 73 (75 f.); *Voigt*, K&R 2014, 325 (326 f.).

310 OVG Schleswig, ZD 2013, 364 (366); so auch *Dammann*, in: Simitis, BDSG, § 1 Rn. 218; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 58 f. m.w.N.; *Plath*, in: Plath, § 1 BDSG Rn. 62; *Kühling*, EuZW 2014, 527 (530); *Piltz*, K&R 2013, 292 (295 f.); *Karg*, ZD 2013, 371 (373); Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 13; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 19 f. Im Ergebnis ist so wohl auch das KG Berlin, ZD 2014, 412 (414 f.) zu verstehen, welches zwar eine ausführliche Auslegung von Art. 4 DSRL vornimmt, letztlich aber § 1 Abs. 5 BDSG – ergänzt um die Ergebnisse der Auslegung des Art. 4 DSRL – als Rechtsgrundlage für die Bestimmung des anwendbaren Rechts heranzieht.

311 Instruktiv: *Haratsch/Koenig/Pechstein*, Europarecht, Rn. 389 ff.

312 Instruktiv: *Haratsch/Koenig/Pechstein*, Europarecht, Rn. 394 ff.

313 OVG Schleswig, ZD 2013, 364 (366); so auch *Dammann*, in: Simitis, BDSG, § 1 Rn. 218; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 58 f. m.w.N.; *Plath*, in: Plath, § 1 BDSG Rn. 62; *Kühling*, EuZW 2014, 527 (531); *Piltz*, K&R 2013, 292 (295 f.); *Karg*, ZD 2013, 371 (373).

2. Umfang der harmonisierenden Wirkung der DSRL

Die praktische Relevanz der Bestimmung des anwendbaren nationalen Rechts ist abhängig vom Umfang der harmonisierenden Wirkung der DSRL.[314] Erwägungsgrund 8 DSRL fordert insoweit ein „gleichwertiges Schutzniveau" in allen Mitgliedstaaten, ergänzt durch das Ziel in Erwägungsgrund 10 DSRL, ein hohes Schutzniveau in der Gemeinschaft herzustellen und damit eine Angleichung nach oben vorzunehmen. Der EuGH stellte hierzu in seiner *Lindqvist*-Entscheidung fest, dass die Harmonisierung durch die DSRL „nicht auf eine Mindestharmonisierung beschränkt [ist]", sondern „zu einer grundsätzlich umfassenden Harmonisierung" führt[315], und bestätigte dies in späterer Rechtsprechung.[316]

Allerdings weist der EuGH auch ausdrücklich darauf hin, dass den Mitgliedstaaten in bestimmten Bereichen ein weiter Handlungsspielraum zukomme und es den Mitgliedstaaten zudem freistehe, den Geltungsbereich der Richtlinie auf weitere, nicht vom Anwendungsbereich der Richtlinie umfasste Bereiche auszudehnen.[317] Trotz des grundsätzlich umfassend harmonisierenden Charakters der DSRL ist es daher den Mitgliedstaaten möglich, strengere Datenschutzvorschriften zu erlassen, soweit ein entsprechender Handlungsspielraum durch Auslegung ermittelt werden kann. Der EuGH konkretisierte dies dahingehend, dass insbesondere Art. 5 DSRL einen solchen Handlungsspielraum aufweist und damit die genaue Ausgestaltung der Voraussetzungen einer zulässigen Datenverarbeitung im Ermessen der Mitgliedstaaten steht.[318] Dieser Handlungsspielraum findet dort seine Grenze, wo die Richtlinie abschließende Regelungen trifft. Beispielsweise statuiert Art. 7 DSRL ausdrücklich, dass eine Datenverarbeitung „lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist". Eine nationale Maßnahme, die die Tragweite eines der in Art. 7 DSRL genannten

---

314 Von einer Vollharmonisierung sprechen in diesem Zusammenhang *Plath*, in: Plath, § 1 BDSG, Rn. 5; *Voigt*, K&R 2014, 325 (325 f.); *Schwartmann/Theodoru*, RDV 2014, 61 (62); *Brühann*, EuZW 2009, 639 (642 ff.), m.w.N, der allerdings bei einzelnen Vorschriften der Richtlinie einen gewissen Regelungsspielraum anerkennt. Der EuGH befasste sich mit der Frage u.a. in den Entscheidungen EuGH, *Lindqvist*, Rs. C-101/01, Slg. 2003, I-12971, Rn. 95 f. = EuR 2004, 291 (304) und EuGH, *„ASNEF/FECEMD"*, Rs. C-468/10 und C-469/10, Rn. 28 ff. = ZD 2012, 33 (34).

315 EuGH, *Lindqvist*, Rs. C-101/01, Slg. 2003, I-12971, Rn. 95 f. = EuR 2004, 291 (304); vgl. auch *Kremer*, RDV 2014, 73 (75); *Brühann*, EuZW 2009, 639 (642 ff.).

316 EuGH, *„ASNEF/FECEMD"*, Rs. C-468/10 und C-469/10, Rn. 28 ff. = ZD 2012, 33 (34).

317 EuGH, *Lindqvist*, Rs. C-101/01, Slg. 2003, I-12971, Rn. 97 f. = EuR 2004, 291 (304 f.); dies vernachlässigt *Voigt*, K&R 2014, 325, 327, welcher aus einer vermeintlichen Vollharmonisierung sogar auf eine direkte Anwendbarkeit des Art. 4 DSRL schließen will, zulasten des § 1 Abs. 5 BDSG.

318 EuGH, *„ASNEF/FECEMD"*, Rs. C-468/10 und C-469/10, Rn. 33 ff. = ZD 2012, 33 (34); zustimmend *Kremer*, RDV 2014, 73 (75); dies entspricht auch Erwägungsgrund 9 der DSRL, wonach die Mitgliedstaaten einen entsprechenden Spielraum besitzen sollten.

Grundsätze verändert, ist demnach unzulässig, während die nähere Ausgestaltung eines der dort genannten Grundsätze im Sinne von Art. 5 DSRL im Ermessen der Mitgliedstaaten liegt.[319]

Angesichts dieser EuGH-Rechtsprechung erweist sich eine Auseinandersetzung um eine pauschale Aussage zur Teil- oder Vollharmonisierung der DSRL als wenig zielführend. Während für die grundsätzlichen Zulässigkeitstatbestände einer Datenverarbeitung von einer umfassenden Harmonisierung auszugehen ist, ist dies bezüglich der konkreten Ausgestaltung der Voraussetzungen der zulässigen Datenverarbeitung aufgrund der verbleibenden Handlungsspielräume der Mitgliedstaaten nicht der Fall. Eine Verschärfung von Schutzstandards in nationalen Regelungen bleibt vielfach möglich, so dass trotz der umfassend harmonisierenden Wirkung nur von einem einheitlichen *Mindest*standard innerhalb der EU und des EWR gesprochen werden kann.[320] Ein Beispiel hierfür ist etwa das Recht auf anonyme Nutzung von Telemedien, welches in § 13 Abs. 6 TMG statuiert ist, aber keine Entsprechung in der DSRL hat und in einigen anderen Mitgliedstaaten – beispielsweise in Irland – nicht existiert.[321] Es ist somit im Einzelfall zu entscheiden, ob von der DSRL abweichende nationale Normen eine zulässige Konkretisierung darstellen oder aber den Handlungsspielraum überschreiten.[322]

Die genaue Bestimmung des konkret anwendbaren Rechts hat daher auch im innereuropäischen Rechtsraum eine hohe praktische Bedeutung, solange die europäische DS-GVO nicht eine weitere Vereinheitlichung des Rechts herbeiführt. Auch mit Anwendbarkeit der DS-GVO werden diese Fragen dort von Relevanz bleiben, wo die DS-GVO den Mitgliedstaaten einen eigenen Regelungsspielraum einräumt und es somit wieder auf nationales Recht ankommt.[323]

3. Möglichkeit einer individuellen Rechtswahl?

In den letzten Jahren gab es wiederholt Diskussionen darüber, ob es sich bei § 1 Abs. 5 BDSG um eine zwingende Kollisionsnorm bzw. kollisionsrechtliches *lex specialis* handelt oder ob die Vertragsparteien die Möglichkeit haben, eine individuelle Rechtswahl im Hinblick auf das

---

319 EuGH, *„ASNEF/FECEMD“*, Rs. C-468/10 und C-469/10, Rn. 35 = ZD 2012, 33 (34); vgl. auch *Plath*, in: Plath, § 1 BDSG, Rn. 5.

320 Vgl. *Caspar*, ZRP 2015, 233 (234); VG Hamburg, ZD 2016, 243 (247); *a*.A. *Voigt*, K&R 2014, 325 (325 f.); *Schwartmann/Theodoru*, RDV 2014, 61 (62); *Brühann*, EuZW 2009, 639 (644).

321 *Caspar*, ZRP 2015, 233 (234).

322 So auch *Kremer*, RDV 2014, 73 (75).

323 Hierzu bereits oben unter C.I.

anwendbare Datenschutzrecht nach Maßgabe von Art. 3 Abs. 1 S. 1 Rom I-VO[324] zu treffen.[325] Nicht zuletzt Facebooks und Googles Nutzungsbedingungen enthalten Rechtswahlklauseln[326], so dass die Frage von hoher praktischer Relevanz ist.

Dabei ist zunächst zwischen zwei Ebenen zu unterscheiden: Die Frage der Rechtswahlmöglichkeit stellt sich primär auf der Ebene des Verhältnisses zwischen dem Anbieter und dem Nutzer des sozialen Netzwerks, da nur hier ein Vertrag geschlossen wird. Hiervon zu unterscheiden ist die Ebene des Verhältnisses des Anbieters zu einer nationalen Aufsichtsbehörde.

Mit der Anmeldung in einem sozialen Netzwerk schließen der Nutzer und der Anbieter einen zivilrechtlichen Nutzungsvertrag ab, wobei der genaue Vertragscharakter umstritten ist.[327] Zwischen ihnen liegt eine „Zivil- und Handelssache" vor, für die grundsätzlich der Anwendungsbereich der Rom I-VO gemäß Art. 1 Abs. 1 und damit auch die Möglichkeit einer Rechtswahl nach Art. 3 Abs. 1 S. 1 Rom I-VO eröffnet ist. Dem steht nicht entgegen, dass das BDSG und TMG öffentlich-rechtliche Regelungen enthalten, da einige der Regelungen sich auch ausdrücklich auf das Verhältnis von Privaten beziehen (beispielsweise §§ 4a, 27-35 BDSG, §§ 11 ff. TMG).[328] Im Rahmen des zivilrechtlichen Verhältnisses ist eine individuelle Rechtswahl also grundsätzlich möglich. Wenn es sich bei dem Nutzer um einen Verbraucher handelt, ist diese Rechtswahlmöglichkeit jedoch insoweit eingeschränkt, als nach Art. 6 Abs. 2

---

[324] VO (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17.6.2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht („Rom I"), ABl. L 177 S. 6.

[325] LG Berlin, ZD 2012, 276 ff.; VG Schleswig, ZD 2013, 245 (245 f.); KG Berlin, ZD 2014, 412 (416 f.); *Piltz*, K&R 2012, 640 ff.; *Polenz*, VuR 2012, 207 (208 f.); *Steinrötter*, MMR 2013, 691ff.; *Jotzo*, MMR 2009, 232 (233 f.); ausdrücklich offen gelassen von VG Hamburg, ZD 2016, 243 (244).

[326] Vgl. z.B. für Facebook: Punkt 15. 1. i.V.m. 16.3 Nr.5 der Nutzungsbedingungen: „Diese Erklärung unterliegt deutschem Recht", https://de-de.facebook.com/legal/terms (Stand 30. Januar 2015); freilich bestreitet Facebook, dass dies auch für das anwendbare Datenschutzrecht gilt und sieht sich insoweit nur irischem Datenschutzrecht verpflichtet, vgl. OVG Schleswig, ZD 2013, 364 (365); VG Hamburg, ZD 2016, 243 (243 ff.); auch Google unterwirft die Nutzung seiner Dienste deutschem Recht, https://www.google.de/intl/de/policies/terms/regional.html.

[327] *Piltz*, Soziale Netzwerke, S. 27 ff; für eine ausführliche vertragstypologische Einordnung vgl. *Redeker*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 12, Rn. 419 ff.; für einen einheitlichen Austauschvertrag, unter Kommerzialisierung des Persönlichkeitsrechts, plädiert *Bräutigam*, MMR 2012, 635 (636); für einen Dienstleistungsvertrag plädieren (auch im Falle der Unentgeltlichkeit) *Jandt/Roßnagel*, MMR 2011, 637 (639 f.), *Dies./Ders.*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 337; von einem „Nutzungsvertrag" sprechen, unter Verweis auf eine bislang fehlende einheitliche Bestimmung der Rechtsnatur, die Datenschutzbeauftragten von Bund und Ländern, in: Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, 2013, S. 15 f.

[328] *Piltz*, K&R 2012, 640 (643); *Weller/Nordmeier*, in: Spindler/Schuster, Art. 9 Rom I-VO, Rn. 14, 17; KG Berlin, ZD 2014, 412 (416).

S. 2 Rom I-VO nicht auf zwingende Normen des Verbraucherschutzes des Aufenthaltsstaates des Verbrauchers verzichtet werden kann.[329]

Im Bereich des Datenschutzrechts gibt es somit prima facie zwei widerstreitende Kollisionsnormen, nämlich einerseits die Regelungen der Rom I-VO mit der Möglichkeit der individuellen Rechtswahl und andererseits Art. 4 Abs. 1 DSRL, welcher in Deutschland in § 1 Abs. 5 BDSG umgesetzt wurde. Ein solcher Konflikt von Verweisungsnormen wird durch Art. 9 Abs. 1 Rom I-VO aufgelöst, indem ein Rekurs auf die Normen der Rom I-VO ausgeschlossen ist, wenn eine sogenannte „Eingriffsnorm" vorliegt. Eingriffsnormen sind Vorschriften, die international zwingende Geltung beanspruchen, ohne Rücksicht auf das anwendbare Sachrecht.[330] Die Eingriffsqualität ist individuell für jede betrachtete Norm zu bestimmen. Indizien für die Qualifizierung als Eingriffsnorm sind hierbei insbesondere wirtschaftspolitische Steuerungsintentionen einer Norm, eine angestrebte Harmonisierung, eine hoheitliche Durchsetzbarkeit der Normen und eine öffentlich-rechtliche Rechtsnatur.[331] § 1 Abs. 5 BDSG wird als Umsetzung von Art. 4 Abs. 1 DSRL in zutreffender Weise ganz überwiegend als Eingriffsnorm und damit abschließende kollisionsrechtliche Regelung eingestuft.[332] Eine Möglichkeit zur individuellen Rechtswahl würde zudem das ausdrücklich in Erwägungsgrund 8 der DSRL genannte Ziel der Harmonisierung des europäischen Datenschutzes konterkarieren. § 1 Abs. 5 S. 1 BDSG stellt daher eine abschließende „innergemeinschaftliche Kollisionsvermeidungsnorm"[333] dar. Für § 1 Abs. 5 S. 2 BDSG ergibt sich der zwingende Anwendungswille des Gesetzes direkt aus dem Wortlaut.

Während also grundsätzlich eine Rechtswahl zwischen dem Anbieter und dem Nutzer erfolgen kann, gilt dies nicht für das anzuwendende Datenschutzrecht. Dieses ist vielmehr ausschließlich nach § 1 Abs. 5 BDSG zu beurteilen. Die gegenteilige Rechtsauffassung des *LG Berlin*, nach

---

329 *Kremer*, RDV 2014, 73 (77); *Piltz*, K&R 2012, 640 (642); *Weller/Nordmeier*, in: Spindler/Schuster, Art. 6 Rom-I-VO, Rn. 1 ff.

330 *Weller/Nordmeier*, in: Spindler/Schuster, Art. 9 Rom I-VO, Rn. 3.

331 *Martiny*, in: MüKo-BGB, Art. 9 Rom I-VO, Rn. 13.

332 Ausführlich: *Piltz*, Soziale Netzwerke im Internet, S. 85 ff.; vgl. auch *Dammann*, in: Simitis, BDSG, § 1 Rn. 197b; *Weller/Nordmeier*, in: Spindler/Schuster, Art. 9 Rom I-VO, Rn. 14, 17; *Kremer*, RDV 2014, 73 (77 f.); *Kremer/Buchalik*, CR 2013, 789 (792); *Piltz*, K&R 2012, 640 (643 f.); *Lindner*, Datenschutzrechtliche Einwilligung, S. 30 ff.; VG Schleswig, ZD 2013, 245 (245 f.); ohne Rekurs auf Art. 9 Abs. 1 Rom I-VO den § 1 Abs. 5 BDSG als „spezialgesetzliche Kollisionsnorm" mit Anwendungsvorrang gegenüber den allgemeinen Kollisionsnormen einordnend: *Jotzo*, MMR 2009, 232 (233); *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 50; *Kartheuser/Klar*, ZD 2014, 500 (501 f.); a.A. KG Berlin, ZD 2014, 412 (416 f.), sowie ohne nähere Begründung LG Berlin, ZD 2012, 276 (278) und *Polenz*, VuR, 2012, 207 (209).

333 *Dammann*, in: Simitis, BDSG, § 1 Rn. 198; vgl. auch *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 50; *Plath*, in: Plath, § 1 BDSG, Rn. 47; *Lindner*, Datenschutzrechtliche Einwilligung, S. 30 ff.

der eine Rechtswahl mangels eines ausdrücklichen Ausschlusses zulässig sei[334], greift insoweit deutlich zu kurz, da der Charakter als Eingriffsnorm übersehen wird. Denselben Vorwurf muss man dem *KG Berlin* machen, das sich zwar ausführlicher mit der Frage der Rechtswahlmöglichkeit beschäftigt, sich aber ebenfalls nicht mit Art. 9 Abs. 1 Rom I-VO auseinandersetzt.[335] Seine Feststellung, dass das BDSG auch privatrechtliche Regelungen enthalte, auf die entsprechend internationales Privatrecht anzuwenden sei, inklusive der Möglichkeit einer Rechtswahl[336], läuft entsprechend ins Leere, da nach eben diesem Regelungsregime eine Rechtswahl gemäß Art. 9 Abs. 1 Rom I-VO ausgeschlossen ist.

Soweit es um ein öffentlich-rechtliches Subordinationsverhältnis zwischen dem Anbieter und einer Aufsichtsbehörde geht, etwa im Rahmen von ordnungsrechtlichen Verfügungen und Bußgeldverfahren, scheidet die Möglichkeit einer Rechtswahl zur Bestimmung des anwendbaren materiellen Rechts dagegen von vorneherein aus. Der Anwendungsbereich der Rom I-VO beschränkt sich gemäß Art. 1 Abs. 1 Rom I-VO auf „Zivil- und Handelssachen". Eine individuelle Rechtswahlvereinbarung für das anwendbare Ordnungsrecht zwischen der Aufsichtsbehörde und dem Anbieter würde dem Grundsatz der Gesetzmäßigkeit der Verwaltung sowie dem Territorialprinzip zuwiderlaufen.[337] Entscheidend ist vielmehr der Anwendungswille des nationalen öffentlichen Rechts, von welchem auszugehen ist, sofern nicht ausdrücklich das (Verwaltungs-)Recht anderer Staaten zum anwendbaren Recht erklärt wird. In diesem Lichte lässt sich § 1 Abs. 5 S. 1 BDSG verstehen, der für die sogleich zu besprechenden Konstellationen die Geltung des BDSG zugunsten anderer mitgliedstaatlicher Regelungen zurücknimmt. Für die Ermittlung der richtigen Ermächtigungsgrundlage zur Beurteilung der Rechtmäßigkeit der hoheitlichen Maßnahme kommt somit keine Rechtswahlmöglichkeit gemäß Art. 3 Abs. 1 S. 1 Rom I-VO in Frage. Die anwendbare Rechtsordnung und hieraus ableitbar die einschlägige Ermächtigungsgrundlage ergibt sich vielmehr aus der Subsumtion des Sachverhalts unter die Kollisionsnorm.[338]

Es ist also jedenfalls missverständlich, wenn das *VG Schleswig* seine Ausführungen zum anwendbaren Recht in der Frage der Rechtmäßigkeit einer Anordnung nach § 38 Abs. 5 BDSG

---

334 LG Berlin, ZD 2012, 276 (278); diesem zustimmend *Polenz*, VuR, 2012, 207 (209). Zustimmung fand das Urteil auch unter (im Verfahren auch als Kläger auftretenden) Verbraucherschützern, die es als „Meilenstein" werteten, ohne sich allerdings mit den kollisionsrechtlichen Fragen auseinanderzusetzen (http://www.vzbv.de/8981.htm); eine entsprechende Auseinandersetzung unterbleibt auch in der zustimmenden Anmerkung von *Solmecke/Baursch*, ZD 2012, 276 (279 f.).

335 KG Berlin, ZD 2014, 412 (416).

336 KG Berlin, ZD 2014, 412 (416).

337 *Steinrötter*, MMR 2013, 691 (692).

338 *Steinrötter*, MMR 2013, 691 (692); vgl. auch VG Hamburg, ZD 2016, 243 (244).

mit der Feststellung beginnt, dass „eine wirksame Rechtswahl des deutschen materiellen Datenschutzrechts“ nicht vorliege.[339] Es ist daher zu begrüßen, dass das *OVG Schleswig* dem nicht folgt, sondern direkt auf § 1 Abs. 5 BDSG als Umsetzung des Art. 4 Abs. 1 lit.a) DSRL als maßgebliche Kollisionsnorm abstellt.[340]

Maßgeblich für die kollisionsrechtliche Bestimmung der Anwendbarkeit des deutschen nationalen Datenschutzrechts ist somit allein § 1 Abs. 5 BDSG, die Möglichkeit einer individuellen Rechtswahl ist abzulehnen. Die Regelungen des BDSG, TMG und TKG finden demnach in vier Fällen Anwendung[341]:

- Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erfolgt im Inland durch eine in Deutschland belegene verantwortliche Stelle[342] (Umkehrschluss aus § 1 Abs. 5 S. 1 BDSG).
- Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erfolgt im Inland durch eine in einem Mitgliedstaat der EU oder einem Vertragsstaat des EWR belegene verantwortliche Stelle, allerdings im Rahmen der Tätigkeit einer Niederlassung in Deutschland (Rückausnahme des § 1 Abs. 5 S. 1 letzter Hs. BDSG).
- Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erfolgt im Inland durch eine nicht in einem Mitgliedstaat der EU oder einem Vertragsstaat des EWR belegene verantwortliche Stelle (§ 1 Abs. 5 S. 2 BDSG).
- Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erfolgt in einem anderen Mitgliedstaat der EU oder einem Vertragsstaat des EWR durch eine in Deutschland belegene verantwortliche Stelle und Niederlassung. Diese Konstellation ist zwar im BDSG nicht ausdrücklich geregelt. Da der entspreche EU- oder EWR-

339 VG Schleswig, ZD 2013, 245 (245 f.); kritisch auch *Steinrötter*, MMR 2013, 691 (691 f.).

340 OVG Schleswig, ZD 2013, 364 (365). Eine individuelle Rechtswahl könnte in ordnungsrechtlichen Verfahren allenfalls dann inzident Bedeutung erlangen, wenn die Rechtmäßigkeit der hoheitlichen Maßnahme davon abhinge, ob im Verhältnis zwischen dem Anbieter und dem Nutzer öffentlich-rechtliche Schutzvorschriften im Rahmen einer wirksamen Rechtswahl *inter partes* abbedungen wurden. Im Ergebnis scheint auch eine solche Möglichkeit zur Rechtswahl indes sehr zweifelhaft, da es dadurch letztlich im Ermessen des Anbieters liegen würde, ob er sich der Geltung ordnungsrechtlicher Normen tatsächlich unterwerfen möchte. Zugleich könnten hoheitliche Befugnisse aufgrund einer privatrechtlichen Vereinbarung begründet werden, weswegen eine solche Möglichkeit zur Rechtswahl vom VG Hamburg, ZD 2016, 243 (244) überzeugend abgelehnt wurde. Diese Frage, die tief in die Thematik des internationalen öffentlichen Rechts hineinreicht, muss an dieser Stelle indes nicht abschließend geklärt werden, da – wie oben bereits gezeigt wurde – auch schon die Möglichkeit der individuellen Rechtswahl bezüglich des anwendbaren Datenschutzrechts zwischen dem Anbieter und dem Nutzer ausscheidet.

341 So bereits systematisiert von *Dammann*, in: Simitis, BDSG, § 1 Rn. 206; vgl. auch *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 54 f.; *Plath*, in: Plath, § 1 BDSG, Rn. 50; *Voigt*, ZD 2014, 15 (16 ff.); Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 13 f.

342 Ausführlich zum Begriff der verantwortlichen Stelle sogleich unter C.II.4.

> Mitgliedsstaat aber gemäß Art. 4 Abs. 1 a) DSRL verpflichtet ist, diese Konstellation vom Anwendungsbereich seines eigenen Rechts auszunehmen, liegt hier eine Regelungslücke vor, so dass § 1 Abs. 5 BDSG richtlinienkonform auszulegen und damit eine Anwendbarkeit des deutschen Datenschutzrechts zu bejahen ist.[343]

Erfolgt die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Inland dagegen durch eine in einem Mitgliedstaat der EU oder einem Vertragsstaat des EWR belegene verantwortliche Stelle und auch im Rahmen der Tätigkeit einer dortigen Niederlassung, so ist eine Anwendbarkeit des BDSG und damit auch des TMG und des TKG ausgeschlossen (§ 1 Abs. 5 S. 1 BDSG). § 1 Abs. 5 S. 1 BDSG statuiert folglich ein modifiziertes Sitzlandprinzip[344], während gemäß § 1 Abs. 5 S. 2 BDSG für nicht in einem Mitgliedstaat der EU oder einem Vertragsstaat des EWR belegene verantwortliche Stellen ein Territorialitätsprinzip zugunsten des deutschen Datenschutzrechts gilt.[345]

4. Bestimmung der „verantwortlichen Stelle“

Zentral für die Bestimmung des anwendbaren Rechts gemäß § 1 Abs. 5 BDSG ist der Begriff der verantwortlichen Stelle.[346] Diese wird in § 3 Abs. 7 BDSG legaldefiniert als „jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“. Die Subsumtion unter diese Vorschrift gestaltet sich indes dort als Herausforderung, wo – wie häufig im Zeitalter digitaler und globaler Datenverarbeitung – eine Verteilung von Arbeitsschritten auf verschiedene Niederlassungen und gegebenenfalls auch Auftragsdatenverarbeiter stattfindet.[347] Tatsächlich kommt es immer seltener vor, dass alle Verarbeitungsschritte an einem einzelnen Ort von einer einzelnen juristischen Entität vorgenommen werden. Dies führt bei weitverzweigten Unternehmensstrukturen mit Niederlassungen und Tochtergesellschaften in unterschiedlichen Ländern zu der Frage, wie viel Einfluss eine Niederlassung auf die Datenerhebung, -verarbeitung und -nutzung haben muss, um als verantwortliche Stelle eingestuft zu werden.

---

343 So auch *Dammann*, in: Simitis, BDSG, § 1 Rn. 206; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 56; *Jotzo*, MMR 2009, 232 (235); vgl. auch *Plath*, in: Plath, § 1 BDSG, Rn. 50.

344 *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 55; *Dammann*, in: Simitis, BDSG, § 1 Rn. 199.

345 *Dammann*, in: Simitis, BDSG, § 1 Rn. 216.

346 Neben der Bestimmung des einschlägigen Rechts ist der Begriff insbesondere auch für die Bestimmung der datenschutzrechtlichen Pflichten von Bedeutung. Hieran hält auch die DS-GVO fest, welche die Definiton aus Art. 2 lit. d) DSRL unverändert in Art. 4 Nr. 7 DS-GVO übernimmt. Hierzu ausführlich unten unter D.I.

347 Vgl. hierzu Art. 29 DatSchGruppe, Stellungnahme 1/2010, WP 169, S. 3 f.

Im Folgenden soll daher am Beispiel von Facebook analysiert werden, wie sich die verantwortliche Stelle im Sinne des § 1 Abs. 5 BDSG bzw. Art. 2 lit.d) DSRL bestimmen lässt. Hierzu gibt es bisher gegensätzliche instanzgerichtliche Urteile. Eine höchstrichterliche Klärung ist noch nicht erfolgt; die Frage ist aber Gegenstand des bereits erwähnten Verfahrens vor dem BVerwG und von der Vorlagefrage an den EuGH umfasst.[348] Es ist zudem zu untersuchen, inwieweit das Urteil des EuGH in der Entscheidung zu dem Suchmaschinenbetreiber *Google* vom Mai 2014[349] auf die Anbieter sozialer Netzwerke übertragbar ist. Während dieses Urteil medienwirksam für die Statuierung eines sogenannten „Rechts auf Vergessen" rezipiert wurde[350], erweisen sich die vom EuGH getätigten Aussagen zur Bestimmung der verantwortlichen Stelle als mindestens ebenso bedeutsam.[351]

Als mögliche verantwortliche Stellen für die Datenverarbeitung deutscher Nutzer kommt zunächst die Muttergesellschaft in den USA, *Facebook Inc.*, in Betracht. Facebook hat zudem eine Niederlassung in Irland, die nach eigenen Angaben für das Geschäft in Europa hauptverantwortlich ist, nämlich die *Facebook Ireland Ltd.*[352] Weitere Niederlassungen existieren in anderen europäischen Mitgliedstaaten, wie beispielsweise die in Deutschland (konkret Hamburg) ansässige *Facebook Germany GmbH*. Diese Nierderlassungen sind hauptsächlich mit der Akquise von Werbekunden und der Verwaltung des Werbeanzeigenmarktes in den jeweiligen Ländern betraut.

Eine Anwendbarkeit deutschen Datenschutzrechts auf Facebook ist zu bejahen, wenn entweder gemäß § 1 Abs. 5 S. 2 BDSG die Muttergesellschaft *Facebook Inc.* als verantwortliche Stelle für die Verarbeitung der Daten deutscher Nutzer einzustufen ist oder die *Facebook Germany GmbH* eine relevante Niederlassung im Sinne von § 1 Abs. 5 S. 1 BDSG darstellt. Ist dagegen die *Facebook Ireland Ltd.* die verantwortliche Stelle und besteht kein hinreichender wirtschaftlich-funktioneller Zusammenhang mit der Tätigkeit der *Facebook Germany GmbH*

---

348 BVerwG, ZD 2016, 393 (393 ff.). Die Anwendbarkeit deutschen Datenschutzrechts verneinen bisher: VG Schleswig, ZD 2013, 245 (245 f.); OVG Schleswig, ZD 2013, 364 (365); VG Hamburg, ZD 2016, 243 (244 ff.); für die Anwendbarkeit deutschen Datenschutzrechts dagegen: KG Berlin, ZD 2014, 412 (414 f.); vgl. auch LG Berlin, ZD 2012, 276 (278), welches allerdings nicht auf die Frage nach der verantwortlichen Stelle eingeht, da es die Anwendbarkeit deutschen Rechts ausschließlich aufgrund einer (entgegen der hier vertretenen Ansicht, s. dazu oben unter C.II.3) für zulässig erklärten individuellen Rechtswahl der Parteien bejaht.

349 EuGH, *Google Spain*, Rs. C-131/12 = JZ 2014, 1009 ff.

350 Vgl. z.B. FAZ v. 13.5.2014, http://www.faz.net/aktuell/wirtschaft/unternehmen/eugh-urteil-ueber-google-recht-auf-vergessen-im-netz-12937165.html; Zeit Online v. 13.5.2014, http://www.zeit.de/digital/datenschutz/2014-05/eugh-urteilt-ueber-recht-auf-vergessenwerden.

351 Hierzu ausführlich unten unter C.II.4.b)bb).

352 Vgl. auch *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 21.

im Sinne des Urteils des EuGH zu *Google Spain*[353], findet gemäß § 1 Abs. 5 S. 1 BDSG irisches Datenschutzrecht Anwendung.

a) Rechtliche vs. tatsächliche Verantwortlichkeit

Der Definitionsansatz des § 3 Abs. 7 BDSG stellt auf den konkreten Datenumgang in Form der Erhebung, Verarbeitung oder Nutzung, bzw. der Vergabe einer Auftragsdatenverarbeitung ab, ist also stark handlungsorientiert. Das BDSG geht somit von der Grundannahme aus, dass es für jede Datenverarbeitung mindestens einen klar bestimmbaren Verantwortlichen gibt, so dass es keine „unverantworteten" Vorgänge geben kann.[354] Dass diese Vorstellung der digitalen Realität noch gerecht wird, wird zunehmend bezweifelt[355] und soll in dieser Arbeit unter D.I.2 noch ausführlicher untersucht werden.

Die europäische DSRL verwendet dagegen den Begriff des „Verantwortlichen" und definiert diesen in Art. 2 lit. d) als „die natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Diese Formulierung wurde wortgleich in Art. 4 Nr. 7 DS-GVO übernommen. Maßgeblich ist mithin nicht, wer direkt mit den Daten umgeht, sondern wer rechtlich oder tatsächlich einen relevanten Einfluss auf die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten hat. Dies ist im Einzelfall anhand funktioneller, faktischer Erwägungen zu beurteilen.[356] Mit Blick auf die zunehmende Komplexität gerade von internetgebundenen Dienstleistungen ist hierbei im Sinne einer effektiven Anwendbarkeit des europäischen Rechts auf eine funktionelle Betrachtungsweise abzustellen, nicht nur eine rein formale.[357] Nur so ist sichergestellt, dass nicht eine Stelle als formal verantwortlich benannt wird, die faktisch nicht in der Position wäre, eine entsprechende

353 EuGH, *Google Spain*, Rs. C-131/12 = JZ 2014, 1009 ff.

354 Vgl. *Dammann*, in: Simitis, BDSG, § 1 Rn. 224.

355 Vgl. z.B. *Dammann*, in: Simitis, BDSG, § 1 Rn. 224.

356 Art. 29 DatSchGruppe, Stellungnahme 1/2010, WP 169, S. 10 ff.; vgl. auch *Martini/Fritzsche*, VerwArch (104) 2013, 449 (461 f.), dort Fn. 6; *Plath/Schreiber*, in: Plath, § 3 BDSG, Rn. 69; *Dammann*, in: Simitis, BDSG, § 3 Rn. 224 ff.; *Wedde*, in: DKWW, § 3 BDSG, Rn. 54; *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 135 f.; *Petri*, ZD 2015, 103 (106).

357 Art. 29 DatSchGruppe, Stellungnahme 1/2010, WP 169, S. 11, 38 ff.; *Kamp*, Personenbewertungsportale, S. 44; *Martini/Fritzsche*, VerwArch (104) 2013, 449 (461 f.), dort Fn. 61; zur begrifflichen Klarstellung sei darauf verwiesen, dass es um eine funktionelle Bestimmung des Einflusses einer juristischen Entität auf die Zwecke und Mittel der Datenverarbeitung geht. Dies ist nicht zu verwechseln mit der früher vorherrschenden funktionalen Betrachtungsweise zur Bestimmung der speichernden Stelle nach § 2 Abs. 3 Nr. 1 i.V.m. § 7 Abs. 1 S. 1 BDSG aF vor der BDSG-Novelle im Jahr 2001, BGBl. I 2001, S. 904 ff.; instruktiv zum funktionalen Stellenbegriff: *Schild*, in: Wolff/Brink, § 3 BDSG, Rn. 109; vgl. auch *Buchner*, in: Taeger/Gabel, § 3 Rn. 54.

Entscheidung über die Zwecke und Mittel der Datenverarbeitung zu treffen.[358] Gegenüber dem handlungsbezogenen Definitionsansatz des § 3 Abs. 7 BDSG erweist sich die funktionelle Herangehensweise der DSRL im Ausgangspunkt als flexibler, birgt damit aber auch größere Rechtsunsicherheiten in sich. Bei der Auslegung der §§ 3 Abs. 7, 1 Abs. 5 BDSG ist sie durch richtlinienkonforme Auslegung zu berücksichtigen.[359]

Mehrere Instanzgerichte haben die *Facebook Ireland Ltd.* als die verantwortliche Stelle für sämtliche personenbezogene Datenverarbeitung von Nutzern aus Deutschland erachtet und entsprechend gemäß § 1 Abs. 5 S. 1 BDSG irisches Datenschutzrecht für anwendbar erklärt.[360] Zur Begründung verweisen sie – neben Angaben von Facebook selbst[361] – auf das Audit des irischen Datenschutzbeauftragten, gemäß welchem das irische Unternehmen innerhalb der *Facebook Gruppe* als einziges die Nutzerdaten Nicht-US-amerikanischer und Nicht-kanadischer Nutzer kontrolliere.[362] Soweit aus dem Audit ersichtlich, beruht aber auch diese Einschätzung ausschließlich auf von *Facebook Ireland Ltd.* selbst getätigten Angaben über die internen Aufgabenverteilungen der Unternehmen der *Facebook Gruppe*, sowie auf vertraglichen Vereinbarungen wie dem „Data Transfer and Processing Agreement" zwischen der *Facebook Ireland Ltd.* und der *Facebook Inc.* aus dem Jahre 2010.[363]

Um die Verantwortlichkeit zu bestimmen, kann indes nicht allein auf eine rein vertragliche Regelung abgestellt werden, da dies zu einer einseitigen Rechtswahlmöglichkeit für den Datenverarbeiter führen und damit die gesetzlichen Kollisionsregeln, die wie bereits festgestellt als Eingriffsnormen ausgestaltet sind, konterkarieren würde. Maßgeblich ist vielmehr die oben beschriebene funktionelle, tatsächliche Betrachtungsweise, mithin die Frage, welchen Einfluss eine Stelle über die Mittel und Zwecke der Datenverarbeitung hat.[364] Eine vertragliche Zuweisung von Verantwortlichkeit ist unbeachtlich, wenn eine andere Stelle entgegen der vertraglichen Vereinbarung den tatsächlich maßgeblichen Einfluss ausübt.[365]

---

358 Art. 29 DatSchGruppe, Stellungnahme 1/2010, WP 169, S. 11; hierzu auch sogleich noch ausführlicher.
359 *Plath/Schreiber*, in: Plath, § 3 BDSG, Rn. 66.
360 VG Schleswig, ZD 2013, 245 (246); OVG Schleswig, ZD 2013, 364 (365 f.); VG Hamburg, ZD 2016, 243 (244 f.).
361 VG Hamburg, ZD 2016, 243 (243).
362 VG Schleswig, ZD 2013, 245 (246); OVG Schleswig, ZD 2013, 364 (366); *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 25, 213.
363 *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 25.
364 KG Berlin, ZD 2014, 412 (415); Art. 29 DatSchGruppe, Stellungnahme 1/2010, WP 169, S. 12; *Piltz*, Soziale Netzwerke, S. 77; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 347.
365 Art. 29 DatSchGruppe, Stellungnahme 1/2010, WP 169, S. 14; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 347.

Im Falle eines Unternehmens wie der *Facebook Gruppe* sind zudem gesellschaftsrechtliche Befugnisse der Muttergesellschaft *Facebook Inc.* zu berücksichtigen, da die *Facebook Ireland Ltd.* ihre 100%ige Tochter ist.[366] Zwar kennt das BDSG kein Konzernprivileg, um Transparenz für die Wahrnehmung von Betroffenenrechten und Kontrollen sicherzustellen.[367] Dies dient insbesondere dem Schutz der innerhalb des Konzerns verarbeiteten Daten: Von einem Unternehmen als verantwortlicher Stelle erhobene Daten dürfen nicht ohne gesetzliche Erlaubnis oder Einwilligung des Betroffenen an eine andere verantwortliche Stelle im Konzern übermittelt werden. Die einzelnen verantwortlichen Stellen sind insofern, trotz ihrer wirtschaftlichen und konzernrechtlichen Verbundenheit, datenschutzrechtlich getrennt zu betrachten. Das insbesondere bei Beschäftigten- oder Kundendaten bestehende wirtschaftliche Interesse an einer Übermittlung der Daten innerhalb des Konzerns muss hinter den Datenschutzinteressen der Betroffenen zurückstehen.[368]

Die Frage nach der verantwortlichen Stelle im Rahmen des § 1 Abs. 5 BDSG ist allerdings unabhängig hiervon zu beurteilen. Anders als bei der Diskussion um das Konzernprivileg geht es nicht primär darum, ob bei der Übermittlung der Daten innerhalb des Konzerns eine eigenständige Datenverarbeitung vorliegt, die entsprechend zu legimitieren wäre. Vielmehr geht es darum, welche Niederlassung als maßgeblicher Anknüpfungspunkt für das anwendbare Datenschutzrecht anzusehen ist, weil sie die funktionelle und faktische Herrschaft über die Datenverarbeitung ausübt. Der Schutzzweck, der der Nichtgewährung des Konzernprivilegs zugrunde liegt, würde umgangen, wenn sich datenverarbeitende Unternehmen durch eine Gründung von Tochterunternehmen wie der *Facebook Ireland Ltd.* dem Datenschutzrecht der Muttergesellschaft entziehen, also sog. „Forum Shopping" betreiben könnten.[369]

Um die verantwortliche Stelle im Sinne des § 1 Abs. 5 BDSG zu bestimmen, genügt es somit nicht, auf die rechtliche Selbstständigkeit einer Tochtergesellschaft zu achten.[370] Vielmehr ist

366 KG Berlin, ZD 2014, 412 (415); Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 6; dies anerkennt auch VG Hamburg, ZD 2016, 243 (243).

367 *Weichert*, in: DKWW, § 3 BDSG, Rn. 59; *Simitis*, in: Simitis, BDSG, § 4c Rn. 61; *Seifert*, in: Simitis, BDSG, § 32 Rn. 116; *Buchner*, in: Taeger/Gabel, § 3 BDSG Rn. 53; *Eßer*, in: Auernhammer, § 3 BDSG, Rn. 72; *Spoerr*, in: Wolff/Brink, § 11 BDSG, Rn. 61; auch die DS-GVO führt grundsätzlich kein Konzernprivileg ein, vgl. *Faust/Spittka/Wybitul*, ZD 2016, 120 (123), eröffnet den Mitgliedstaaten aber in Art. 88 Abs. 2 DS-GVO einen Regelungsspielraum für die Datenübermittlung im Beschäftigungskontext innerhalb einer Unternehmensgruppe.

368 *Simitis*, in: Simitis, BDSG, § 4c Rn. 61 ff.; *Seifert*, in: Simitis, BDSG, § 32 Rn. 116 ff.; vgl. auch *Spoerr*, in: Wolff/Brink, § 11 BDSG, Rn. 61.

369 Vgl. *Nguyen*, ZD 2015, 265 (267).

370 So aber ohne zwischen § 1 Abs. 5 BDSG und anderen Verwendungen des Begriffs der verantwortlichen Stelle zu differenzieren *Weichert*, in: DKWW, § 3 BDSG, Rn. 59.

ein entsprechender Wirtschaftsteilnehmer gegebenenfalls als Einheit anzusehen, wenn es sich bei unterschiedlichen Stadien der Datenverarbeitung insgesamt um ein einheitliches Geschäftsmodell handelt.[371] Dem hat sich auch der EuGH in seinem Urteil zu *Google Spain* angeschlossen, indem er feststellte, dass Tätigkeiten wie der Betrieb der Suchmaschine und der Verkauf individueller Werbeflächen „untrennbar miteinander verbunden" seien, auch wenn diese durch unterschiedliche Niederlassungen ausgeübt würden. Dabei sei es inakzeptabel, wenn „die Verarbeitung personenbezogener Daten, die zum Betrieb der Suchmaschine ausgeführt wird, den in der Richtlinie 95/46 vorgesehenen Verpflichtungen und Garantien entzogen" werde.[372] Obwohl es im geltenden Datenschutzrecht kein Konzernprivileg gibt, sind datenverarbeitende Konzerne daher insoweit als eine Einheit zu betrachten, als dies bei einer funktionell-wirtschaftlichen Betrachtung ihrer Tätigkeiten geboten ist, um ein „forum shopping" durch Gründung verschiedener verantwortlicher Stellen zu verhindern.[373]

Wegen der gesellschaftsrechtlichen Beherrschung ist es nicht ausgeschlossen, dass die *Facebook Inc.* wesentliche Entscheidungsprozesse an sich ziehen kann.[374] Ein vertragliches Abkommen wie das „Data Transfer and Processing Agreement", welches die Tochtergesellschaft umfassend zur Verarbeitung der Daten berechtigt, ist für sich genommen noch nicht geeignet, eine hinreichende faktische Verantwortlichkeit dieser Tochtergesellschaft zu begründen. Das rechtliche Abkommen sagt isoliert noch nichts darüber aus, inwiefern der 100%igen Tochtergesellschaft auch faktisch die Möglichkeit zukommt, über Zwecke und Mittel der Datenverarbeitung unabhängig vom Willen der Muttergesellschaft zu entscheiden. Es ist nicht erkennbar, inwieweit die *Facebook Ireland Ltd.* auf eigene Datenverarbeitungsstrukturen, insbesondere eigene Programmierung zurückgreifen und

---

371 So auch schon Schlussanträge des Generalanwalts, *Jääskinen*, v. 25.6.2013, Rs. C-131/12, Rn. 65 ff.; ablehnend: *Pauly/Ritzer/Geppert*, ZD 2013, 423 (424 ff.).

372 EuGH, *Google Spain*, Rs. C-131/12, Rn. 56, 58 = JZ 2014, 1009 (1013).

373 Hierzu auch noch ausführlich unter C.II.4.b); vgl. zum Problem des Forum Shoppings auch *Karg*, ZD 2013, 371 (373). Je nach konkreter Ausgestaltung kann dies dazu führen, dass eine formal untergeordnete Niederlassung entweder als verantwortliche Stelle anzusehen ist oder nicht. Im Fall von *Google Spain SL* und – wie sogleich zu zeigen wird – der *Facebook Germany GmbH*, führt die funktionell-wirtschaftliche Betrachtung zu einer „Aufwertung" der formal untergeordneten Niederlassung zur verantwortlichen Stelle mit der Konsequenz der Anwendbarkeit des dortigen nationalen Datenschutzrechts. In Fällen wie der *Facebook Ireland Ltd.*, welche im Sinne dieser Betrachtung gerade keine verantwortliche Stelle darstellt (auch hierzu sogleich) und der *Facebook Inc.* als Muttergesellschaft, kann sich die Muttergesellschaft indes nicht durch die Gründung von solchen Zweiggesellschaften einem ggf. strengeren nationalen Datenschutzrecht entziehen, welches ansonsten über § 1 Abs. 5 S. 2 BDSG bzw. Art. 4 lit. c) DSRL zur Anwendung käme. Abzustellen ist also – wie bereits zuvor und auch noch nachfolgend in diesem Kapitel analysiert – auf die konkret untersuchte Datenverarbeitung, die faktischen Machtverhältnisse bezüglich derselben und die funktionell-wirtschaftliche Bedeutung dieser Verarbeitung für das Geschäftsmodell des Konzerns.

374 KG Berlin, ZD 2014, 412, 415; *Kremer*, RDV 2014, 73 (81); vgl. auch Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 6 f.

Einfluss auf die Plattformgestaltung und damit die Eingabemöglichkeit von Daten durch Nutzer nehmen kann.[375] Vielmehr wird insbesondere in den jährlichen Geschäftsberichten von 2014 und 2015 für die American Securities and Exchange Commission (SEC) ausdrücklich darauf hingewiesen, dass es sich bei der Facebookgruppe um ein einheitliches Unternehmen handele und sämtliche letztgültige Entscheidungsgewalt in der Hand des Geschäftsführers von Facebook Inc. liege.[376]

Zudem ist es nicht ausgeschlossen, dass dieses Abkommen jederzeit durch einen Gesellschafterbeschluss der Muttergesellschaft eingeschränkt oder ganz aufgehoben wird.[377] Natürlich ist es nicht zwangsläufig so, dass eine Muttergesellschaft diese Möglichkeiten der Einflussnahme auch nutzt.[378] Es ist allerdings im Wesentlichen eine Frage der Beweislast, ob der Muttergesellschaft eine konkrete Einflussnahme nachgewiesen werden muss oder vielmehr diese sich entlasten muss. Für die Beschwerdeführer, Datenschutzbehörden und Gerichte dürfte es im Einzelfall sehr schwer sein, einen hinreichenden Einblick in die Unternehmensabläufe zu erlangen, um zu überprüfen, ob entgegen einer entsprechenden vertraglichen Vereinbarung maßgeblicher Einfluss auf die Mittel und Zwecke der Datenverarbeitung durch die Muttergesellschaft genommen wird. Der Vorrang der faktischen Verantwortlichkeit vor der vertraglichen liefe damit häufig leer. Stattdessen würde großen Unternehmen die Möglichkeit eröffnet, durch vertragliche Gestaltungen der Datenverarbeitung mit ihren Tochterunternehmen eine einseitige Rechtswahl zu treffen, die dem Prinzip der faktischen und funktionellen Verantwortlichkeit zuwiderläuft. Dieses Ergebnis kann vom Gesetzgeber nicht gewollt gewesen sein. Daher ist jedenfalls in 100%igen Beherrschungssituationen wie zwischen der *Facebook Inc.* und der *Facebook Ireland Ltd.* zunächst von einer Verantwortlichkeit der Muttergesellschaft auszugehen. Es obliegt der Muttergesellschaft, diesen Anschein durch Beibringung hinreichender Beweise zu widerlegen. Sie muss neben einer vertraglichen Verantwortlichkeit auch die tatsächliche funktionelle Verantwortlichkeit der

375 KG Berlin, ZD 2014, 412 (415); *Piltz*, Soziale Netzwerke, S. 78 f.

376 Facebook Inc., Form 10-k für die amerikanische SEC, abgegeben am 29.01.2015, für den Zeitraum bis 31.12.2014, S. 67: „Our chief operating decision-maker is our Chief Executive Officer who makes resource allocation decisions and assesses performance based on financial information presented on a consolidated basis. There are no segment managers who are held accountable by the chief operating decisionmaker, or anyone else, for operations, operating results, and planning for levels or components below the consolidated unit level. Accordingly, we have determined that we have a single reportable segment and operating unit structure."; dieselbe Formulierung findet sich in dem Form 10-k, abgegeben am 28.1.2016, für den Zeitraum bis 31.12.2015, S. 66; vgl. auch Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 6 f.

377 KG Berlin, ZD 2014, 412 (415); *Kremer*, RDV 2014, 73 (81).

378 Vgl. *Kartheuser/Klar*, ZD 2014, 500 (503).

Tochtergesellschaft im Sinne einer nachhaltigen und unabhängigen Entscheidungsfreiheit bezüglich der Datenverarbeitung begründen.[379]

Verallgemeinert ist also jene Stelle verantwortlich im Sinne der Kollisionsnormen, die funktionell und tatsächlich über die Mittel und Zwecke der Datenverarbeitung entscheidet. In Bezug auf Facebook ist entgegen des irischen Auditberichts und der Entscheidungen des VG und OVG Schleswig nicht davon auszugehen, dass dies bei der *Facebook Ireland Ltd.* der Fall ist. Vielmehr sprechen sowohl die einheitliche Plattformgestaltung als auch die gesellschaftsrechtlichen Beherrschungsverhältnisse dafür, dass die Muttergesellschaft *Facebook Inc.* in den USA einen erheblichen Einfluss hinsichtlich der Mittel und Zwecke der Datenverarbeitung behält. Eine Einstufung der *Facebook Ireland Ltd.* als (allein) Verantwortlicher und damit als nach § 1 Abs. 5 S. 1 BDSG maßgebliche verantwortliche Stelle ist deswegen abzulehnen.[380] Vielmehr sind die *Facebook Inc.* und die *Facebook Ireland Ltd.* allenfalls als gemeinsam verantwortliche Stellen anzusehen, wenn man nicht sogar eine Alleinverantwortlichkeit der *Faecbook Inc.* bejahen will. Da die *Facebook Inc.* nicht in einem Mitgliedstaat der EU bzw. des EWR ansässig ist, aber hier im Inland personenbezogene Daten erhebt, wenn Nutzer an ihren Endgeräten das soziale Netzwerk Facebook nutzen und dort Datenspuren hinterlassen, fände gemäß § 1 Abs. 5 S. 2 BDSG deutsches Datenschutzrecht Anwendung.[381]

Zu berücksichtigen ist an dieser Stelle indes auch die *Facebook Germany GmbH* mit Sitz in Hamburg. Dieser kommt zwar – soweit ersichtlich – keine eigene Entscheidungsbefugnis hinsichtlich der Mittel und Zwecke der Datenverarbeitung zu. Ihre Tätigkeit ist allerdings wirtschaftlich untrennbar mit der Tätigkeit der verantwortlichen *Facebook Inc.* verbunden. Eine Anwendbarkeit deutschen Datenschutzrechts könnte sich daher auch aus § 1 Abs. 5 S. 1 BDSG ergeben, wenn es sich hierbei um eine Niederlassung im Sinne der Vorschrift handelt. Dies soll im Folgenden untersucht werden.

---

379 So im Ergebnis auch schon *Kremer*, RDV 2014, 73 (81); a.A. *Kartheuser/Klar*, ZD 2014, 500 (503), die nur bei Vorliegen von konkreten Anhaltspunkten für eine Einflussnahme der Muttergesellschaft deren Verantwortlichkeit bejahen wollen.

380 So auch schon *Piltz*, Soziale Netzwerke, S. 78 f.; KG Berlin, ZD 2014, 412 (415); *Kremer*, RDV 2014, 73 (81); ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 19; vgl. auch Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 7.

381 So auch KG Berlin, ZD 2014, 412 (415); *Piltz*, Soziale Netzwerks, S. 79; *Maisch*, Informationelle Selbstbestimmung, S. 184; *Karg/Thomsen*, DuD 2012, 729 (734); ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 19 f.; *Nolte*, ZRP 2011, 236 (239); vgl. auch *Kremer*, RDV 2014, 73 (80 ff.); ausführlich hierzu auch noch unten unter C.II.4.c).

b) „Im Rahmen der Tätigkeit einer Niederlassung“

Das soeben diskutierte Element der Verantwortlichkeit wird durch ein Sitzprinzip der verantwortlichen Stelle ergänzt. In der Regelung des § 1 Abs. 5 S. 1 BDSG folgt dies schon aus dem Wortlaut der verantwortlichen „Stelle“. Art. 4 lit. a) DSRL wird insoweit noch deutlicher und verlangt ausdrücklich eine Verarbeitung von Daten, die „im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden“. Spätestens seit dem Google-Urteil des EuGH ist klargestellt, dass diesem Kriterium eine erhebliche eigenständige Bedeutung im Zusammenhang mit der Bestimmung des Verantwortlichen zukommt; sie erschöpft sich keinesfalls in einer Abgrenzung zu reinen reinen Softwarezugriffen aus dem Ausland und damit den Regelungen des § 1 Abs. 5 S. 2 BDSG, bzw. Art. 4 lit. c) DSRL.

Der EuGH stufte die ausschließlich für Werbeaquise zuständige Niederlassung der *Google Spain SL* wurde als verantwortliche Stelle für die deutlich weitergehende Verarbeitung personenbezogener Daten im Zusammenhang mit der Erstellung von Suchergebnissen durch die *Google Inc.* in den USA ein.[382] Das Urteil führt dazu, dass es zur Bestimmung der verantwortlichen Stelle nicht länger ausreicht zu betrachten, wer die tatsächliche und funktionelle Entscheidungsbefugnis über Mittel und Zwecke der gesamten Datenverarbeitung hat. Vielmehr müssen für die Verantwortungszuweisung auch untergeordnete Entscheidungsbefugnisse berücksichtigt werden, soweit diese wirtschaftlich unverzichtbar für die größere, gesamte Datenverarbeitung sind. Für die Frage des anwendbaren Rechts auf soziale Netzwerke ist die Entscheidung wegweisend, da nicht zuletzt Facebook und Google mit der *Google Spain SL* vergleichbare Niederlassungen in Deutschland unterhalten. Wie oben unter C.I. bereits dargelegt wurde, könnte sie zudem auch unter Geltung der DS-GVO von erheblicher Bedeutung für die Bestimmung der zuständigen Aufsichtsbehörde sein. Im Folgenden soll daher das Merkmal „im Rahmen der Tätigkeit einer Niederlassung“ analysiert werden und sodann die Übertragbarkeit der Erkenntnisse des Google-Urteils insbesondere auf die deutsche Niederlassung der *Facebook Germany GmbH* geprüft werden.

aa) Begriff der „Niederlassung“

Der Begriff der „Niederlassung“ ist weder im BDSG noch in der europäischen DSRL definiert; in Erwägungsgrund 19 ist lediglich festgehalten, dass eine Niederlassung die „effektive und

[382] EuGH, *Google Spain*, Rs. C-131/12, Rn. 60 = JZ 2014, 1009 (1013); vgl. hierzu auch *Spindler*, JZ 2014, 981 (984).

tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung“ voraussetzt. Der EuGH hat diese Kriterien in seiner Entscheidung zu *Google Spain* aufgegriffen und ihr Vorliegen unproblematisch bejaht.[383] Diese Rechtsprechung hat er im Oktober 2015 in seiner Entscheidung zu *Weltimmo* bestätigt.[384] Zur Begriffsklärung kann weiterhin auf die Rechtsprechung des EuGH zur Niederlassungsfreiheit gemäß Art. 49 AEUV zurückgegriffen werden, wonach für eine feste Niederlassung „ein ständiges Zusammenwirken von persönlichen und Sachmitteln“[385] erforderlich ist, mithin eine Struktur, „die von der personellen und sachlichen Ausstattung her eine autonome Erbringung der betreffenden Dienstleistungen ermöglicht“[386]. Der bloße Standort eines Servers ist somit nicht entscheidend. Maßgeblich ist vielmehr, ob in einer Niederlassung menschliche Tätigkeiten zur Erbringung der Dienstleistung erfolgen und ob im Rahmen dieser Tätigkeiten persönliche Daten verarbeitet werden.[387] Dieses Erfordernis ist gerade bei im Internet angebotenen Leistungen flexibel auszulegen und kann unter bestimmten Umständen sogar schon bei Vorhandensein nur eines einzigen Vertreters in einem Mitgliedstaat erfüllt sein.[388]

Ob die Verarbeitung „im Rahmen der Tätigkeiten“ der Niederlassung erfolgt, ist anhand eines funktionellen Ansatzes zu beurteilen, der sowohl den weiteren rechtlichen Kontext, als auch den tatsächlichen Umfang der Tätigkeiten berücksichtigt.[389] Hierbei kann auch eine geringfügige Tätigkeit ausreichend sein.[390] Je nach Verarbeitungsschritt und Involvierung unterschiedlicher Niederlassungen können für unterschiedliche Verarbeitungsschritte somit verschiedene nationale Rechtsordnungen zur Anwendung kommen.[391]

383 EuGH, *Google Spain*, Rs. C-131/12, Rn. 48 f. = JZ 2014, 1009 (1012 f.).
384 EuGH, *Weltimmo*, Rs. C-230/14, Rn. 29 ff. = ZD 2015, 580 (582); ebenfalls bestätigt in EuGH, *Amazon EU*, Rs. C-191/15, Rn. 75 ff. = EuZW 2016, 754 (758).
385 EuGH, *Berkholz*, Rs. C-168/84, Rn. 19 = UR 1985, 225 (228).
386 EuGH, *ARO Lease*, Rs. C-190/95, Rn. 16 = UR 1998, 185 (186).
387 Art. 29 DatSchGruppe, Stellungnahme 8/2010, WP 179, S. 14; *Piltz*, Soziale Netzwerke, S. 72 f.; *Dammann*, in: Simitis, BDSG, § 1 Rn. 203; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 55; *Jotzo*, MMR 2009, 232 (235); Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 14.
388 EuGH, *Weltimmo*, Rs. C-230/14, Rn. 29 f. = ZD 2015, 580 (582); vgl. auch EuGH, *Amazon EU*, Rs. C-191/15, Rn. 75 ff. = EuZW 2016, 754 (758).
389 Art. 29 DatSchGruppe, Stellungnahme 8/2010, WP 179, S. 19 ff.; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 55.
390 EuGH, *Weltimmo*, Rs. C-230/14, Rn. 31= ZD 2015, 580 (582); EuGH, *Amazon EU*, Rs. C-191/15, Rn. 78 ff. = EuZW 2016, 754 (758).
391 Art. 29 DatSchGruppe, Stellungnahme 8/2010, WP 179, S. 16; *Piltz*, Soziale Netzwerks, S. 74.

bb) Das EuGH Urteil zu Google Spain

Der EuGH betont in seinem Urteil zu *Google Spain*, dass Art. 4 Abs. 1 lit. a) DSRL nicht verlangt, dass die Tätigkeit auch tatsächlich „von" dieser Stelle selbst ausgeführt wird.[392] Eine enge Auslegung der Formulierung „im Rahmen der Tätigkeiten einer Niederlassung", die nur örtliche Aspekte in Betracht zieht und im Kontext digitaler Arbeitsteilung und der damit einhergehenden Diffusion von Verantwortlichkeit und Zuständigkeit verfehlt wäre, scheidet damit aus. Der EuGH stellt vielmehr fest, dass Zweigniederlassungen oder Tochtergesellschaften von Suchmaschinenbetreibern, die in einem Mitgliedstaat zur Förderung des Verkaufs von Werbeflächen der Suchmaschine an Einwohner dieses Staats gegründet werden, einen hinreichenden Tätigkeitsumfang aufweisen können, um im Rahmen der Tätigkeiten der Niederlassung Datenverarbeitung zu betreiben.[393] Die Analyse, welche Werbung zu den Nutzerinteressen am besten passt und daher zu der Suche eingeblendet werden soll, stelle eine mit der eigentlichen Datenverarbeitung, nämlich der Strukturierung der Ergebnisse der Suchanfrage, welche durch *Google Inc.* vorgenommen werde, „in dem betreffenden Mitgliedstaat untrennbar […] verbunden[e]" Tätigkeit dar.[394] Denn erst durch einen effizienten Einsatz der Werbeflächen lasse sich eine wirtschaftliche Rentabilität der Suchmaschine erreichen.[395] Die Auswahl der mit den Suchbegriffen verknüpften Suchergebnisse durch *Google Inc.* sei daher unmittelbar mit der Auswahl der Werbeanzeigen durch die *Google Spain SL* verknüpft und präsentiere sich stets auf der gleichen Webseite. Die Datenverarbeitung bei der Werbetätigkeit der *Google Spain SL* lasse sich daher nicht von der im Rahmen der Zusammenstellung des Suchergebnisses erfolgenden Verarbeitung personenbezogener Daten durch *Google Inc.* trennen.[396] Vielmehr erfolge sie im Rahmen der Tätigkeit der Niederlassung im Sinne von Art. 4 Abs. 1 lit. a) DSRL.[397] Der bisherige funktionelle Ansatz zur Bestimmung der verantwortlichen Stelle wird hierdurch im Interesse eines effektiven Grundrechtsschutzes zu einer funktionell-wirtschaftlichen Betrachtung erweitert.

---

392 EuGH, *Google Spain*, Rs. C-131/12, Rn. 52 = JZ 2014, 1009 (1013); bestätigt in EuGH, *Weltimmo*, Rs. C-230/14, Rn. 35 = ZD 2015, 580 (582).

393 EuGH, *Google Spain*, Rs. C-131/12, Rn. 55 ff. = JZ 2014, 1009 (1013); zustimmend: *Dammann*, in: Simitis, BDSG, § 1 Rn. 202; *Weichert*, ZD 2014, 605 (608); Art. 29 DatSchGruppe, Update of Opinion 8/2010, WP 179 update, S. 4 ff.

394 EuGH, *Google Spain*, Rs. C-131/12, Rn. 56 = JZ 2014, 1009 (1013).

395 EuGH, *Google Spain*, Rs. C-131/12, Rn. 56 = JZ 2014, 1009 (1013).

396 Vgl. EuGH, *Google Spain*, Rs. C-131/12, Rn. 28 ff., 41 = JZ 2014, 1009 (1011 f.)

397 EuGH, *Google Spain*, Rs. C-131/12, Rn. 60 = JZ 2014, 1009 (1013); so auch bereits *Martini/Fritzsche*, VerwArch (104) 2013, 449 (461 f.), dort Fn. 61; a.A.: *Pauly/Ritzer/Geppert*, ZD 2013, 423 (424 f.).

In dieser Auslegung wird der EuGH durch den Generalanwalt unterstützt. Auch dieser hatte zuvor festgestellt, dass eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung vorliegt, wenn „diese Niederlassung als Bindeglied zwischen dem Referenzierungsdienst und dem Werbemarkt des betreffenden Mitgliedsstaats fungiert", sich also „für die Vermarktung und den Verkauf von Werbeflächen der Suchmaschine […] an die Bewohner dieses Staates richtet".[398] Die in der Literatur betonte Abweichung des EuGH von den Ausführungen des Generalanwalts[399] betrifft dagegen die vorgelagerte Frage, ob Suchmaschinenbetreiber in der Zusammenstellung von Inhalten Dritter überhaupt für die damit zusammenhängende Verarbeitung personenbezogener Daten verantwortlich sind oder ob sich ihre Tätigkeit lediglich in einer „völlig passiven Vermittlungsfunktion"[400] erschöpft. Hier überzeugt der EuGH, indem er betont, dass der Suchmaschinenbetreiber zwar keinen Einfluss auf die Originaldaten in den Quellen Dritter nimmt, aber in der Indexierung und Zusammenstellung der zuvor dezentralen Inhalte eine eigenständige Datenverarbeitung liegt, die jedem Nutzer ermöglicht, ohne großen Aufwand über fremde Personen „ein mehr oder weniger detailliertes Profil" erstellen zu können.[401]

Die funktionell-wirtschaftliche Betrachtung stellt einen effektiven Regulierungsansatz dar, um global agierende Dienstleistungsunternehmen im Internet zu regulieren und sicherzustellen, dass sie ihre Umsätze zu vergleichbaren gesetzlichen Bedingungen erzielen wie „Offline-Unternehmen" in den entsprechenden Ländern. Ein Unternehmen, das sein Geschäftsmodell weitgehend auf die Verarbeitung von Daten stützt, ist für seine zentrale Datenverabeitung nicht an ein bestimmtes Land gebunden. Wie im Fall von Google reicht es vielmehr aus, untergeordnete Niederlassungen in speziellen Ländern zu gründen und diese Niederlassungen vor Ort Daten sammeln zu lassen, diese Daten dann an den Hauptsitz zu versenden und erst dort gewinnbringend zu verarbeiten. Nur aufgrund der einfachen Übermittlung von Daten ist es nicht erforderlich, eine Infrastruktur zur Datenverarbeitung direkt in dem speziellen Land, aus dem die Gewinne letztlich erzielt werden und an deren Bevölkerung sich das Angebot eigentlich richtet, vorzuhalten. Ohne die wirtschaftlich-funktionelle Betrachtung könnte das nationale Recht die Geschäfte eines solchen Unternehmens nicht effektiv regulieren, obwohl diese im Hoheitsgebiet des Rechts agieren, was einen massiven Steuerungsverlust bedeuten würde. Insbesondere im Vergleich zu offline agierenden Unternehmen, die nicht derart global

398 Schlussanträge des Generalanwalts *Jääskinen*, v. 25.6.2013, Rs. C-131/12, Rn. 67 f.
399 Vgl. z.B. *Boehme-Neßler*, NVwZ 2014, 825 (827); *Spindler*, JZ 2014, 981 (982); *Buchholtz*, AöR 2015, 121 (140 f.).
400 So ausdrücklich Schlussanträge des Generalanwalts *Jääskinen*, v. 25.6.2013, Rs. C-131/12, Rn. 85.
401 EuGH, *Google Spain*, Rs. C-131/12, Rn. 28, 37, 80 = JZ 2014, 1009 (1011 ff.); zustimmend auch *Buchholtz*, AöR 2015, 121 (143); *Skouris*, NVwZ 2016, 1359 (1361 f.).

arbeiten können, sondern eine lokale Präsenz haben müssen, ist nicht einsichtig, warum Dienstleistungsunternehmen des Internets derart privilegiert werden sollten.

Die weite Auslegung des Begriffs der „verantwortlichen Stelle“ ist auch aus Sicht eines effektiven Grundrechtsschutzes der Internetnutzer zu begrüßen, zumindest solange es keine umfassendere Vereinheitlichung des Datenschutzrechts innerhalb der EU durch die geplante DS-GVO gibt.[402] Diese Auslegung ermöglicht eine differenziertere Anwendung nationaler Datenschutzgesetze auf Niederlassungen, die das Angebot eines Internetunternehmens spezifisch auf nationale Nutzerbedürfnisse und -interessen zuschneiden und durch einen entsprechenden nationalfokussierten Auftritt auch den Eindruck für die Nutzer erwecken, dass sie sich in ihrem „eigenen“ nationalen Rechtsraum aufhalten.

Diese weite Auslegung ist daher geeignet, die Problematik des „Forum Shoppings“ zu verringern, indem Unternehmen die Möglichkeit genommen wird, sich die günstige Rechtslage eines anderen Staates durch eine Niederlassung dort zu sichern, aber zugleich mit (untergeordneten) Niederlassungen im eigentlichen Mitgliedstaat präsent zu sein und dort ein wirtschaftlich perfekt abgestimmtes Angebot zu schaffen.[403] Das ansonsten drohende datenschutzrechtliche „race to the bottom“ der Mitgliedstaaten widerspräche dem übergeordneten Ziel der DSRL gemäß ihrem Erwägungsgrund 10, „ein hohes Schutzniveau“ in der Gemeinschaft sicherzustellen.[404]

Kritiker werfen der weiten Auslegung der Forumulierung „Rahmen der Tätigkeiten einer Niederlassung“ durch den Generalanwalt und den EuGH vor, dass sie die Systematik von Art. 4 lit. a) DSRL und Art. 4 lit. c) DSRL verletze und für Art. 4 lit. c) DSRL kein Anwendungsbereich mehr verbleibe.[405] Sie führe dazu, dass eine Niederlassung überhaupt keine Datenverarbeitung mehr ausführen müsse, um eine Verantwortlichkeit zu begründen, was die Wortlautgrenze deutlich verletze und daher abzulehnen sei.[406]

Dem ist nicht zu folgen. Die Formulierung „im Rahmen der Tätigkeit“ bietet grundsätzlich genug Raum, um auch eine funktionell-wirtschaftliche Zusammengehörigkeit zu berücksichtigen. Zudem verbleibt als Anwendungsbereich für Art. 4 lit. c) DSRL zumindest der Fall, in dem ein außerhalb der EU und des EWR ansässiges Unternehmen in Mitgliedstaaten

---

402 Zustimmend *Nolte*, NJW 2014, 2238 (2239); *Spindler*, JZ 2014, 981 (984 f.); *Boehme-Neßler*, NVwZ 2014, 825 (827); kritisch zur praktischen Umsetzbarkeit des Urteils mit Blick auf die Durchsetzung von Löschungsrechten *Ziebarth*, ZD 2014, 394 (398).

403 Vgl. auch Art. 29 DatSchGruppe, Update of Opinion 8/2010, WP 179 update, S. 6 f.

404 So auch Art. 29 DatSchGruppe, Update of Opinion 8/2010, WP 179 update, S. 7.

405 *Kremer*, RDV 2014, 73 (80).

406 *Kremer*, RDV 2014, 73 (80).

belegene Mittel nutzt, um personenbezogene Daten zu erheben oder zu verarbeiten und dabei keinerlei Niederlassung in diesem Staat hat. Die Regelung läuft somit keinesfalls vollkommen leer, auch wenn man dem EuGH folgt.

cc) Übertragbarkeit der Google Spain Entscheidung auf die Facebook Germany GmbH

Es spricht viel dafür, dass die soeben skizzierten Feststellungen des EuGHs in der Entscheidung zu *Google Spain* auf die *Facebook Germany GmbH* zu übertragen sind, mit der Folge, dass wegen dieser Niederlassung in Deutschland deutsches Datenschutzrecht anwendbar ist.[407] Die Aufgaben dieser Niederlassung sind gemäß der von Facebook selbst übermittelten Angaben im Rahmen des Audits 2011 folgendermaßen zu umschreiben:

> *„FB-I* [= Facebook Ireland Ltd., Anm. d. Verfasserin] *is supported by a network of small local offices scattered across the EU. These offices, which operate under the control and direction of FB-I, seek to promote Facebook, and Facebook advertisements, within their geographical and linguistic area of responsibility.*
>
> *These offices have no role in the development or maintenance of the platform or the control of user data. Their functions are limited to the sale of advertising, local PR and, in limited cases, addressing queries from local app developers. In the context of carrying out these duties, these offices may process a limited amount of user data relating to the pages of advertisers and prospective advertisers pursuant to processing agreements entered into with FB-I.*
>
> *Offices are located in Amsterdam, Hamburg, London, Madrid, Milan, Paris, Stockholm.“*[408]

Vor der Google-Entscheidung des EuGH wurde verbreitet davon ausgegangen, dass der auf Vermarktung und Optimierung von Werbeflächen für deutschsprachige Nutzer beschränkte Tätigkeitsbereich keine Verantwortlichkeit im Sinne des § 1 Abs. 5 S. 1 BDSG auslöse.[409] Als Anknüpfungspunkt für die Anwendbarkeit deutschen Datenschutzrechts kam die *Facebook Germany GmbH* daher nur insoweit in Frage, als sie eigenständig im Rahmen ihrer Tätigkeit

---

407 So auch *Caspar*, ZD 2015, 12 (14); *Petri*, ZD 2015, 103 (104); *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (2); *Spindler*, JZ 2014, 981 (985); *Ziebarth*, ZD 2014, 394 (399); *Beyvers/Herbrich*, ZD 2014, 558 (561); vgl. auch *Hoffmann-Riem*, Innovation und Recht, S. 655; vgl. entsprechend für die Anwendbarkeit belgischen Datenschutzrechts aufgrund der vergleichbaren Facebook Belgium SPRL in Belgien: Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 10 ff., 14; a.A. VG Hamburg, ZD 2016, 243 (246 f.).

408 *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 215.

409 VG Schleswig, ZD 2013, 245 (246 f.); OVG Schleswig, ZD 2013, 364 (366); damals noch *Dammann*, in: Simitis, BDSG, 7. Auflage 2011, § 1 Rn. 220; mittlerweile geändert *Dammann*, in: Simitis, BDSG, § 1 Rn. 202; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 58; *Piltz*, Soziale Netzwerke, S. 75; *Maisch*, Informationelle Selbstbestimmung, S. 181; *Karg*, ZD 2013 371 (374) m.w.N.; *Karg/Thomsen*, DuD 2012, 729 (733); implizit ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 19; vgl. zusammenfassend auch *Spindler*, JZ 2014, 981 (984).

personenbezogene Daten verarbeitete, also beispielsweise Persönlichkeitsprofile nutzte, um diese konkreten Werbeangeboten zuzuordnen.[410] Eine umfassende Verantwortlichkeit für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung des sozialen Netzwerks – welche im Zweifel von der *Facebook Ireland Ltd.* nach Vorgaben der *Facebook Inc.* vorgenommen wurde – konnte der *Facebook Germany GmbH* nicht zugewiesen werden. Entsprechend konnte auf diese umfassende Datenverarbeitung nur dann deutsches Datenschutzrecht Anwendung finden, wenn nicht die *Facebook Ireland Ltd.* als hierfür (allein-)verantwortliche Stelle eingestuft wurde, sondern die *Facebook Inc.* in den USA, vgl. § 1 Abs. 5 S. 2 BDSG, bzw. Art. 4 lit. c) DSRL.[411]

Die Artikel-29 Datenschutzgruppe plädierte schon 2010 dafür, den „Rahmen der Tätigkeit" mit einem funktionellen Ansatz zu bestimmen.[412] Dieser beschränkte sich damals allerdings darauf, „theoretischen Bewertungen" – und damit möglichen Umgehungskonstruktionen – der Beteiligten weniger Gewicht beizumessen und stattdessen auf das tatsächliche Maß zu achten, in welchem Niederlassungen personenbezogene Daten im Rahmen ihrer Tätigkeiten verarbeiteten, und „ihr praktisches Vorgehen und ihre Interaktion" zu berücksichtigen.[413] Letztlich sollte ausschlaggebend für die Ermittlung der für Art. 4 lit. a) DSRL relevanten Niederlassung sein, „ob die betreffende Organisation effektiv und tatsächlich derartige Tätigkeiten ausübt".[414] In Bezug auf die *Facebook Germany GmbH* hätte sich diese Tätigkeit auf die oben beschriebene Vermarktung und den Verkauf von Werbung und die damit zusammenhängende stark eingeschränkte Verarbeitung personenbezogener Daten im Auftrag der *Facebook Ireland Ltd*. beschränkt.

Genau hier setzt die Argumentation des EuGH an, der den funktionellen Ansatz auf die Frage ausweitet, ob die Tätigkeit der Niederlassung und des Suchmaschinenbetreibers „untrennbar miteinander verbunden" sind, um eine wirtschaftliche Nutzung der Suchmaschine zu ermöglichen.[415] Das Argument des EuGH läuft darauf hinaus, dass diese untrennbare Verbindung zu einer Vermischung bzw. gar Verschmelzung der faktisch getrennten Tätigkeitsbereiche führt: Im Interesse eines effektiven Grundrechtsschutzes könne es nicht angehen, dass ein für die Datenverarbeitung Verantwortlicher sich der Geltung von

410 Vgl. hierzu allgemein Art. 29 DatSchGruppe, Stellungnahme 8/2010, WP 179, S. 14, 16 u. 36.
411 Hierzu schon oben unter C.II.4.a) und sogleich noch unter C.II.4.c).
412 Art. 29 DatSchGruppe, Stellungnahme 8/2010, WP 179, S. 36.
413 Art. 29 DatSchGruppe, Stellungnahme 8/2010, WP 179, S. 36; nunmehr allerdings gänzlich dem EuGH folgend: Art. 29 DatSchGruppe, Update of Opinion 8/2010, WP 179 update, S. 2 ff.
414 Art. 29 DatSchGruppe, Stellungnahme 8/2010, WP 179, S. 36.
415 EuGH, *Google Spain*, Rs. C-131/12, Rn. 56 = JZ 2014, 1009 (1013).

Datenschutzstandards entziehe, indem er in einer untergeordneten Niederlassung in einem Mitgliedstaat nur sehr begrenzt personenbezogene Daten verarbeite, die Ergebnisse dieser Datenverarbeitung aber unverzichtbar für die wirtschaftliche Fortführung der eigentlich verantwortlichen Niederlassung seien.[416] Dieser Auslegung hat sich die Artikel-29 Datenschutzgruppe nunmehr in einer Aktualisierung ihrer Stellungnahme 8/2010 umfassend angeschlossen.[417]

Übertragen auf Facebook und die *Facebook Germany GmbH* müsste die Frage also lauten, ob auch hier die gezielte Vermarktung von Werbung durch die *Facebook Germany GmbH* (und vergleichbarer Niederlassungen) erst die Rentabilität des sozialen Netzwerks ermöglicht. Für Google – mittlerweile „Alphabet" – lag der Anteil der Werbungeinnahmen am Gesamtumsatz im Jahr 2013 bei 91,04%.[418] Bei Facebook lag dieser Anteil im gleichen Jahr mit 88,74% nur geringfügig niedriger. Sonstige Einnahmequellen für Facebook waren insbesondere Zahlungen und Gebühren für Apps, wie etwa das Spiel „FarmVille".[419] 2014 lag der Anteil der Werbeeinnahmen am Gesamtumsatz Facebooks bereits bei 92,19%, 2015 bei 95,26%.[420] Angesichts der stetig sinkenden Nutzung des sozialen Netzwerks von Desktop-PCs aus, die aktuell immer noch hauptverantwortlich für die Einnahmen durch Spiele-Apps ist, rechnete Facebook bereits im Jahr 2014 mit einer weiteren Verringerung des proportionalen Anteils dieser Einnahmen und damit einer weiteren proportionalen Zunahme der Werbeeinnahmen.[421] Facebook stellt zudem selbst ausdrücklich fest, dass nahezu sämtliche Einnahmen über die Ermöglichung personalisierter Werbung generiert werden, durch welche Händler gezielt mit potentiellen Kunden in Kontakt treten können.[422]

---

416 EuGH, *Google Spain*, Rs. C-131/12, Rn. 58 = JZ 2014, 1009 (1013).

417 Art. 29 DatSchGruppe, Update of Opinion 8/2010, WP 179 update, S. 2 ff.

418 https://investor.google.com/financial/tables.html: Bei einem Gesamtumsatz von 55,52 Milliarden (Mrd.) US-Dollar im Jahr 2013 stammten 50,55 Mrd. US-Dollar Umsatz aus Werbeeinnahmen. 2014 hat sich der Gesamtumsatz auf 66 Mrd. US-Dollar erhöht, wobei 59,62 Mrd. US-Dollar aus Werbeeinnahmen stammen, was einem Anteil von 90,34% entspricht.

419 Facebook Annual Report 2013, S. 46: 2013 erzielte Facebook Gesamteinnahmen von 7,87 Mrd. US-Dollar. Hiervon stammten 6,99 Mrd. US-Dollar aus Werbeeinnahmen (= 88,74%) und 886 Mio. US-Dollar aus Gebühren und Zahlungen für Apps und Ähnliches (= 11,26%).

420 Facebook Inc., Form 10-k für die amerikanische SEC, abgegeben am 29.01.2015 für den Zeitraum bis 31.12.2014, S. 62; Facebook Annual Report 2014, S. 43; Facebook Annual Report 2015, S. 42. Wie sich den Jahresberichten a.a.O. entnehmen lässt, lag 2014 gegenüber 2013 eine Steigerung des Umsatzes um 58% vor, da u.a. 11,49 Mrd. US-Dollar aus Werbeeinnahmen erzielt wurden bei einem Gesamtumsatz von 12,47 Mrd. US-Dollar. Dies ist insbesondere auf eine Steigerung des Werbeumsatzes um 4,5 Mrd. US-Dollar bzw. 65% zurückzuführen. 2015 erfolgte eine erneute Umsatzsteigerung um 44% auf einen Gesamtumsatz von 17,93 Mrd. US-Dollar, wovon 17,079 Mrd. US-Dollar auf Werbeeinnahmen entfielen.

421 Facebook Inc., Quarterly Report Filed 10/30/14 for the Period Ending 09/30/14, S. 31.

422 Facebook Annual Report 2013, S. 36.

Spätestens mit den Zahlen aus dem Jahr 2015 kann nicht mehr bezweifelt werden, dass die gezielte Vermarktung von Werbung die Rentabilität des Netzwerks begründet. Durch den Wert der personalisierten Werbung stellen die unmittelbaren Tätigkeiten der *Facebook Germany GmbH* eine wirtschaftlich untrennbar mit den Tätigkeiten der *Facebook Inc.* verbundene Einheit dar: Die *Facebook Germany GmbH* könnte ohne die Datenverarbeitung der *Facebook Inc.* ihre Werbung nicht vermarkten, und letztere könnte ohne erstere (und vergleichbare Niederlassungen) das soziale Netzwerk nicht wirtschaftlich betreiben.[423] Dass Facebook als Anbieter eines sozialen Netzwerks andere Dienste anbietet als der Suchmaschinenbetreiber Google, steht einer Übertragung der vom EuGH aufgestellten Grundsätze nicht entgegen, da die genaue Tätigkeit Googles insoweit nicht von Bedeutung für die Entscheidung war.

Soweit das *VG Hamburg* eine Übertragbarkeit der Rechtsprechung mit dem Argument ablehnt, der EuGH habe sich nur mit einer Abgrenzung einer Niederlassung innerhalb der Europäischen Union, nämlich *Google Spain*, und der in den USA ansässigen *Google Inc.* befasst, nicht aber mit der Abgrenzung von zwei Niederlassungen innerhalb der Europäischen Union[424], kann dies nicht überzeugen. Zum einen ist festzuhalten, dass die *Google Inc.* eine mit der *Facebook Ireland Ltd.* jedenfalls im Grundsatz vergleichbare europäische Hauptniederlassung in Irland betreibt, welche „in gewissem Umfang" den europäischen Betrieb koordiniert und über weitere Datenzentren und Niederlassungen unter anderem in Belgien und Finnland verfügt.[425] Zum anderen ist es zwar richtig, dass der EuGH seine Entscheidung unter anderem mit dem Anliegen eines effektiven Grundrechtsschutzes begründet hat, um eine Umgehung der Anwendbarkeit der DSRL zu verhindern.[426] Der – zutreffende – Kern seines Arguments liegt aber in der gegenseitigen Zurechnung von Datenverarbeitungsvorgängen aufgrund einer wirtschaftlichen Untrennbarkeit und damit einem funktionell-wirtschaftlichen Verantwortlichkeitsbegriff.[427] Dass eine solche auch im Falle der *Facebook Germany GmbH* im Verhältnis zu den anderen Unternehmen Facebooks vorliegt, erkennt das *VG Hamburg* indes ohne Weiteres an.[428] Eine Abgrenzung danach, mit der Tätigkeit welcher Niederlassung „die streitige Datenverarbeitung am engsten verbunden ist"[429], ist nach dieser holistischen Betrachtung indes logisch ausgeschlossen. Die Konsequenz des Urteils des EuGH zu *Google Spain* ist, dass es gerade

423 So auch bereits *Martini/Fritzsche*, VerwArch (104) 2013, 449 (461 f.), dort Fn. 61.
424 VG Hamburg, ZD 2016, 243 (246).
425 Schlussanträge des Generalanwalts *Jääskinen*, v. 25.6.2013, Rs. C-131/12, Rn. 62; vgl. auch Art. 29 DatSchGruppe, Update of Opinion 8/2010, WP 179 update, S. 5.
426 EuGH, *Google Spain*, Rs. C-131/12, Rn. 58 = JZ 2014, 1009 (1013); VG Hamburg, ZD 2016, 243 (246).
427 EuGH, *Google Spain*, Rs. C-131/12, Rn. 56 ff. = JZ 2014, 1009 (1013); Art. 29 DatSchGruppe, Update of Opinion 8/2010, WP 179 update, S. 3 ff.
428 VG Hamburg, ZD 2016, 243 (246).
429 So VG Hamburg, ZD 2016, 243 (246 f.).

nicht auf die lokale Verantwortlichkeit – und damit die Entscheidungskompetenz über Zwecke und Mittel – einer Niederlassung in Bezug auf die konkrete Datenverarbeitung ankommt, sondern die Bedeutung der konkreten Datenverarbeitung in Bezug auf das Geschäftsmodell des gesamten Konzerns. Für diese Beurteilung kann es indes nicht von Belang sein, ob es weitere Niederlassungen innerhalb der Europäischen Union gibt oder nicht.

Hierdurch kann es zwar zu der Situation kommen, dass auf die Datenverarbeitung innerhalb der Union unterschiedliches nationales Datenschutzrecht zur Anwendung kommt. Somit können zusätzliche Kosten für datenverarbeitende Unternehmen entstehen, die durch die Statuierung des Sitzprinzips des Art. 4 lit. a) DSRL bzw. § 1 Abs. 5 S. 1 BDSG ursprünglich vermieden werden sollten.[430] Allerdings liegt es in der Hand eines jeden Unternehmens, sich dieser Rechtsfolge zu entziehen, indem es auf die Gründung entsprechender untergeordneter Niederlassungen in anderen Mitgliedstaaten verzichtet. Es gibt keinen Anspruch darauf, zugunsten eines bestimmten profitablen Geschäftsmodells von unbequemen Rechtsfolgen verschont zu bleiben, so dass diese Konsequenz hinzunehmen ist.[431]

Die vom EuGH vorgenommene funktionell-wirtschaftliche Auslegung der Formulierung „im Rahmen der Tätigkeiten einer Niederlassung“ ist somit auch für das Unternehmen Facebook und vergleichbare soziale Netzwerke relevant. Sie führt konkret zur vollständigen Anwendbarkeit deutschen Datenschutzrechts auf sämtliche Verarbeitungen personenbezogener Daten durch die *Facebook Inc.* bzw. die *Facebook Ireland Ltd.*, welche in einem wirtschaftlich untrennbaren Zusammenhang zur Datenverarbeitung durch die deutsche Niederlassung der *Facebook Germany GmbH* stehen.[432]

Solange die DS-GVO noch nicht anwendbar ist, findet mithin gemäß § 1 Abs. 5 S. 1 BDSG deutsches Datenschutzrecht auf soziale Netzwerke Anwendung, wenn sie die Datenverarbeitung durch eine verantwortliche Stelle im Inland vornehmen lassen. Es findet darüber hinaus Anwendung, wenn ein soziales Netzwerk zumindest eine Niederlassung im Inland unterhält, welche personenbezogene Daten im Rahmen ihrer Tätigkeit verarbeitet,

---

430 Vgl. VG Hamburg, ZD 2016, 243 (246 f.).

431 So auch Art. 29 DatSchGruppe, Update of Opinion 8/2010, WP 179 update, S. 6 f.

432 So nun auch *Caspar*, ZD 2015, 12 (14); *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (2); vgl. entsprechend für die Anwendbarkeit belgischen Datenschutzrechts aufgrund der vergleichbaren Facebook Belgium SPRL in Belgien: Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 10 ff., 14; a.A. VG Hamburg, ZD 2016, 243 (246 f.); jedenfalls unklar *Plath/Schreiber*, in: Plath, § 3 BDSG, Rn. 69, welche zwar davon ausgehen, dass nach dem *Google*-Urteil eine „Niederlassung“ im Sinne des Art. 4 Abs. 1 lit. a) DRSL vorliege (so auch *Plath*, a.a.O., § 1 BDSG, Rn. 52), diese aber keine verantwortliche Stelle im Sinne von § 3 Abs. 7 BDSG darstelle, ohne hierbei eine mögliche gespaltene Begriffsauslegung gegenüber § 1 Abs. 5 S. 1 BDSG zu begründen.

soweit diese Datenverarbeitung in einem untrennbaren wirtschaftlich-funktionellen Zusammenhang mit dem Betrieb des sozialen Netzwerks steht.

Auch nach Anwendbarkeit der DS-GVO bleibt die Frage der datenschutzrechtlichen Verantwortlichkeit der *Facebook Germany GmbH* von hoher Relevanz, da sich eine Haupt-)Zuständigkeit der deutschen Datenschutzbehörden ergeben kann, sofern die *Facebook Germany GmbH* als relevante Niederlassung im Rahmen des Art. 56 Abs. 2 DS-GVO zu betrachten ist.[433]

c) Verwendung von im Mitgliedsstaat belegenen Mitteln

Wenn die verantwortliche Stelle keine Niederlassung in der EU bzw. dem EWR hat, kann zur Begründung der Anwendbarkeit europäischen Datenschutzrechts gemäß Art. 4 lit. c) DSRL an die Verwendung von im Mitgliedsstaat belegenen Mitteln angeknüpft werden.[434] Diese Regelung wurde in der Novelle des § 1 Abs. 5 S. 2 BDSG nur mangelhaft umgesetzt. Während die Richtlinie auch einen Rückgriff auf „automatisierte oder nicht automatisierte Mittel" als Anknüpfungspunkt statuiert, fehlt diese Variante in der deutschen Umsetzung.[435] Stattdessen spricht § 1 Abs. 5 S. 2 BDSG nur von der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Inland. Dem ist durch eine richtlinienkonforme extensive Auslegung des § 1 Abs. 5 BDSG zu begegnen.[436]

Als in Mitgliedstaaten belegene Mittel kommen insbesondere Endnutzergeräte wie Smartphones oder PCs in Betracht. Ein Zurückgreifen auf diese Mittel zum Zwecke der Verarbeitung personenbezogener Daten soll nach überzeugender Ansicht vieler Autoren und Gerichte bereits dann vorliegen, wenn auf dem Endgerät eine Nutzeridentifikation etwa durch das Ablegen von Cookies erfolgt.[437] Problematischer ist dagegen die Frage, wie es sich mit frei zugänglichen Websites verhält, in die Nutzer Daten eintragen können, die aber nicht direkt auf den PC des Nutzers zur Datenerhebung zurückgreifen, also insbesondere keine (dauerhaften) Cookies ablegen. Ob und inwieweit bereits hierin ein entsprechender Rückgriff auf in der Union

433 Hierzu bereits ausführlich oben unter C.I.3.

434 Vgl. VG Schleswig, ZD 2013, 245 (246 f.); *Piltz*, Soziale Netzwerke, S. 74; Art. 29 DatSchGruppe, Stellungnahme 8/2010, WP 179, S. 23 f., 34.

435 *Kremer*, RDV 2014, 73 (75); *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 58 f.; *Plath*, in: Plath, § 1 BDSG, Rn. 62.

436 Hierzu schon oben unter C.II.

437 KG Berlin, ZD 2014, 412 (414 f.); *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 59; *Plath*, in: Plath, § 1 BDSG, Rn. 66; *Piltz*, K&R 2013, 292 (295); *Kroschwald*, ZD 2013, 388 (394); *Pauly/Ritzer/Geppert*, ZD 2013, 423 (425); *Karg/Thomsen*, DuD 2012, 729 (734); *Jotzo*, MMR 2009, 232 (236).

belegene Mittel vorliegt, ist nicht abschließend geklärt, wird aber häufig verneint.[438] Auch der EuGH hat diese Frage im Google-Urteil offen gelassen, da er bereits eine Verantwortlichkeit nach Art. 4 lit. a) DSRL bejaht hatte.[439]

In dieser Arbeit wurde bereits gezeigt, dass für Facebook eine Verantwortlichkeit nach § 1 Abs. 5 S. 1 BDSG zu bejahen ist, soweit es verantwortliche Niederlassungen im europäischen Raum gibt. Soweit solche nicht vorhanden sind, stellt eine aktive Aufforderung an europäische Nutzer, ihre Daten mit ihren Endgeräten in soziale Netzwerke einzustellen bei gleichzeitiger Ablage von Cookies auf diesen Endgeräten[440], jedenfalls einen Rückgriff auf in Mitgliedstaaten belegene Mittel dar. Entsprechend wäre in richtlinienkonformer Auslegung unproblematisch eine Verantwortlichkeit nach § 1 Abs. 5 S. 2 BDSG gegeben. Die weitergehende Frage, ob auch das bloße Eintragen von Daten in einer frei zugänglichen Webseite mit einem in einem Mitgliedstaat belegenen Endgerät bereits die Voraussetzungen von § 1 Abs. 5 S. 2, bzw. Art. 4 lit. c) DSRL erfüllt, soll hier daher ausgeklammert und der weiteren Forschung überlassen werden.

III. Nationale materielle Anwendbarkeit des BDSG, TMG und TKG auf Daten in sozialen Netzwerken nach bisheriger Rechtslage

Das deutsche Datenschutzrecht teilt sich in allgemeine Regelungen im BDSG und den Landesdatenschutzgesetzen sowie zahlreiche bereichsspezifische Datenschutzregelungen in Spezialgesetzen. Das BDSG stellt daher nur eine subsidiäre Regelung des Datenschutzes dar. Es ist nur einschlägig, wenn nach Art der Daten keine spezielleren Regeln des TMG oder des TKG eingreifen.[441] Der Anwendungsbereich des TKG und des TMG wird insbesondere durch die Klassifikation von Verkehrsdaten (§§ 3 Nr. 30, 96 TKG), Bestandsdaten (§ 14 TMG) und Nutzungsdaten (§ 15 TMG) bestimmt. Die Einordnung der gesetzlich nicht ausdrücklich geregelten Inhaltsdaten ist umstritten. Um den jeweiligen Umfang der materiellen Anwendbarkeit der Gesetze auf soziale Netzwerke bestimmen zu können, ist es somit erforderlich, nach den Datenarten zu differenzieren. Aus den zuvor dargelegten Gründen erfolgt auch hier eine Analyse nach der bisher geltenden Rechtslage.[442]

---

438 *Dammann*, in: Simitis, BDSG, § 1 Rn. 223 ff.; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 59; vgl. auch *Nolte*, NJW 2014, 2238 (2240); *Jotzo*, MMR 2009, 232 (236).

439 EuGH, *Google Spain*, Rs. C-131/12, Rn. 61 = JZ 2014, 1009 (1013).

440 Vgl. hierzu und zu anderen Mechanismen der Nutzeridentifikation bereits oben unter B.II.2.b)aa).

441 *Schmidt*, in: Taeger/Gabel, § 1 BDSG, Rn. 33 ff.; *Dix*, in: Simitis, BDSG, § 1 Rn. 158 ff. m.w.N.

442 Vgl. oben unter C. und C.I.

1. Verkehrsdaten

Verkehrsdaten i.S.v. §§ 3 Nr. 30, 96 TKG sind solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Es handelt sich dabei um Daten, die für den Übermittlungsvorgang an sich benötigt werden, also insbesondere die Kennungsnummern der beteiligten Anschlüsse, Beginn und Ende der jeweiligen Verbindung nach Datum und Uhrzeit und ggf. die Menge der übermittelten Datenmengen, soweit die Entgelte hiervon abhängen (vgl. § 96 Abs. 1 TKG). Die Aufzählung in § 96 Abs. 1 Nr. 1-4 TKG ist hierbei grundsätzlich abschließend.[443] Der abschließende Charakter wird allerdings durch die weite Formulierung des § 96 Abs. 1 Nr. 5 TKG aufgeweicht, welcher als Auffangtatbestand die Erhebung und Verwendung „aller sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendigen Verkehrsdaten“ gestattet, um zukünftigen technologischen Entwicklungen flexibel begegnen zu können.[444]

Verkehrsdaten stellen überaus sensible Daten dar, da sie eine exakte Verfolgung der Kommunikation von Nutzern ermöglichen. Auch wenn die genauen Inhalte eines Telefongesprächs oder einer Internetkommunikation nicht gespeichert werden, zeigen diese Daten, wer wann mit wem wie lange an welchem Ort kommuniziert hat. Dies offenbart unter anderem Einblicke in den Tagesablauf einer Person, in ihre soziale Vernetztheit und ihre Beziehung zu bestimmten Personen. Eine Verwendung der Daten stellt somit einen erheblichen Eingriff in die Rechte der Betroffenen dar, insbesondere in das Fernmeldegeheimnis (Art. 10 Abs. 1 GG, § 88 Abs. 2 TKG).[445] Sie ist daher nur unter den engen Voraussetzungen des § 96 Abs. 1, S. 2 und Abs. 3 TKG zulässig. Der dortige Verweis auf die durch andere gesetzliche Vorschriften begründeten Zwecke flexibilisiert die Verwendung der Verkehrsdaten insbesondere zugunsten der Strafverfolgungs- und Sicherheitsbehörden. Zu nennen sind hier insbesondere die Vorschriften der §§ 100g, 100h StPO, §§ 8 Abs. 8, 10 BVerfSchG, § 10 Abs. 3 MADG, § 8 Abs. 3a BNDG und § 101 Abs. 2 und 9 UrhG.[446] Ob dieser Zusatz tatsächlich den Bestimmtheitsanforderungen genügt, die vom BVerfG in der Kontenabruf-Entscheidung aufgestellt wurden, also insbesondere den Kreis der zugriffsberechtigten Behörden hinreichend präzise festlegt[447], ist zweifelhaft.[448] Diese Frage soll hier aber nicht vertieft werden.

---

443 *Munz*, in: Taeger/Gabel, § 96 TKG, Rn. 5.
444 *Munz*, in: Taeger/Gabel, § 96 TKG, Rn. 9.
445 *Munz*, in: Taeger/Gabel, § 96 TKG, Rn. 1, 3; vgl. auch *Jenny*, in: Plath, § 96 TKG, Rn. 2.
446 *Munz*, in: Taeger/Gabel, § 96 TKG, Rn. 12.
447 Vgl. hierzu grundlegend BVerfGE 118, 168 (186 ff.).
448 *Munz*, in: Taeger/Gabel, § 96, TKG, Rn. 12, m.w.N.

In Bezug auf soziale Netzwerke stellt sich für das TKG zunächst die Frage der Anwendbarkeit. Gemäß § 91 Abs. 1 TKG finden die Datenschutzbestimmungen des TKG Anwendung bei der Erhebung und Verwendung von „Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken". Abzugrenzen ist hierbei zum Anwendungsbereich des TMG. Dieser ist gemäß § 1 Abs. 1 TMG „für alle elektronischen Informations- und Kommunikationsdienste" eröffnet, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien)". Die Abgrenzung zwischen Telekommunikationsdiensten und Telemediendiensten kann im Einzelfall erhebliche Schwierigkeiten bereiten.[449] Letztlich sind unter Telekommunikationsdiensten im Sinne des § 3 Nr. 24 TKG „Dienste *der* Kommunikation" zu verstehen, die sich auf den technischen Vorgang der Telekommunikation beschränken, also die Übertragung von Signalen über Telekommunikationsnetze.[450] Bei Telemedien handelt es sich dagegen um „lediglich mit Hilfe der Telekommunikation angebotene Dienstleistungen"[451], mithin „Dienste *durch* Telekommunikation"[452]. Es erfolgt somit eine funktionell-inhaltliche Abgrenzung.[453] Soweit Telekommunikationsdienste „überwiegend" Signale über Telekommunikationsnetze übertragen, zusätzlich aber auch inhaltliche Dienste anbieten, sind das TKG und das TMG parallel anzuwenden. Hinsichtlich der Datenschutzvorschriften ordnet indes § 11 Abs. 3 TMG einen weitgehenden Vorrang der Regelungen des TKG an.[454]

Soziale Netzwerke bieten eine Vielzahl unterschiedlicher Funktionen an, von denen einige – wie etwa die Möglichkeit eines Live-Chats – je nach der konkreten technischen Ausgestaltung als Telekommunikationsdienste eingeordnet werden könnten.[455] Dies betrifft insbesondere das Versenden von privaten Nachrichten oder Chat-Mitteilungen. Konkrete Verkehrsdaten sind

449 Ausführlich am Beispiel von Instant Messengern wie WhatsApp: *Schneider*, ZD 2014, 231 (235 ff.).
450 *Kremer*, CR 2012, 438 (440); *Karg/Fahl*, K&R 2011, 453 (456); *Munz*, in: Taeger/Gabel, Einf TKG, Rn. 10.
451 *Munz*, in: Taeger/Gabel, Einf TKG, Rn. 10; vgl. auch *Moos*, in: Taeger/Gabel, Einf TMG, Rn. 5 f.
452 *Karg/Fahl*, K&R 2011, 453 (456).
453 *Kremer*, CR 2012, 438 (440); *Karg/Fahl*, K&R 2011, 453 (456); *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 4.
454 *Munz*, in: Taeger/Gabel, Einf TKG, Rn. 10; kritisch hinsichtlich der Bestimmtheit des Merkmals „überwiegend" in § 11 Abs. 3 TMG: *Schneider*, ZD 2014, 231 (236 f.).
455 *Kremer*, CR 2012, 438 (440); *Redeker*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 12, Rn. 430; vgl. auch *Moos*, in: Taeger/Gabel, Einf TMG, Rn. 5; *Schneider*, ZD 2014, 231 (237).

hierbei insbesondere Absender, Empfänger, Datum und Uhrzeit der Nachricht, da ohne diese eine Zustellung der Nachricht an einen bestimmten Empfänger nicht möglich ist.[456] Zwar werden rein technisch betrachtet keine Signale übertragen, wie etwa beim Versand einer Email, sondern die Daten auf derselben Plattform des sozialen Netzwerks gespeichert und lediglich für den Sender und den Empfänger freigeschaltet.[457] Die Funktion und die Wirkungsweise entsprechen allerdings jener des klassischen Emailversands, welcher als Signalübertragung den Datenschutzbestimmungen des TKG unterliegt.[458] Die technische Übermittlung von Informationen steht im Vordergrund, während eine inhaltliche Auswertung oder Verknüpfung als Teil der Leistungserbringung in aller Regel ausbleibt.[459] In Bezug auf diese isolierten Funktionen, bei denen es primär um eine Verarbeitung von Verkehrsdaten geht, ist daher von einer parallelen Anwendbarkeit des TKG und TMG auszugehen, wobei auf die Einschränkungen des § 11 Abs. 3 TMG zu achten ist.[460]

Schwerpunktmäßig werden soziale Netzwerke allerdings als Informations- und Kommunikationsplattformen genutzt, auf denen Informationen gespeichert, zum Abruf bereitgestellt und verknüpft werden. Somit steht nicht die reine Datenübertragung, sondern die inhaltliche Leistung im Vordergrund, so dass auf den Gesamtdienst sozialer Netzwerke nach ganz herrschender Ansicht das TMG, nicht aber das TKG anzuwenden ist.[461]

---

456 *Karg/Fahl*, K&R 2011, 453 (457).

457 *Karg/Fahl*, K&R 2011, 453 (456); *Redeker*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 12, Rn. 430; vgl. zu dieser Abgrenzung auch *Spindler/Nink*, in: Spindler/Schuster, § 11 TMG, Rn. 28.

458 *Redeker*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 12, Rn. 419, 430 f.; *Schneider*, ZD 2014, 231 (234); *Hullen/Roggenkamp*, in: Plath, § 11 TMG Rn. 8, 19; *Spindler/Nink*, in: Spindler/Schuster, § 11 TMG, Rn. 28. Insbesondere ist anders als beispielsweise bei Skype, welches keinen Telekommunikationsdienst darstellt, aber vergleichbar zu einer Email oder Messenger Diensten wie WhatsApp eine zeitlich asynchrone Kommunikation möglich.

459 Facebook versichert, dass es die privat ausgetauschten Nachrichten nicht für Zwecke des Targeted Advertising analysiert und auswertet, *Irish Data Protection Commissioner*, Report of Re-Audit, 21.09.2012, S. 18. Selbst wenn dennoch eine inhaltliche Analyse erfolgen sollte, stellt dies jedenfalls nicht die vom Nutzer gewünschte Leistung dar. Die so gewonnenen Erkenntnisse würden dem Nutzer nicht mitgeteilt und wären daher auch nicht prägend für Facebooks Leistung an die Nutzer. Die technische Übertragung von Informationen steht damit bei Funktionen wie dem Live-Chat im Vordergrund.

460 *Kremer*, CR 2012, 438 (440); *Karg/Fahl*, K&R 2011, 453 (456).; *Hullen/Roggenkamp*, in: Plath, § 11 TMG Rn. 8.

461 *Piltz*, Soziale Netzwerke, S. 49, 60; *Kremer*, CR 2012, 438 (440); *Moos*, in: Taeger/Gabel, Einf TMG, Rn. 5; *Hullen/Roggenkamp*, in: Plath, § 11 TMG Rn. 6; *Weichert*, JBÖS 2012/2013, 379 (384); *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 341 f.; *Redeker*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 12, Rn. 415 f., 429; *Karg/Fahl*, K&R 2011, 453 (456); *Jotzo*, MMR 2009, 232 (234); vgl. auch auf europarechtlicher Ebene Art. 29 DatSchGruppe, Stellungnahme 5/2009, WP 163, S. 5.

2. Bestandsdaten

§ 14 Abs. 1 TMG definiert Bestandsdaten als „personenbezogene Daten eines Nutzers […], [die] für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind." Sie werden daher auch teilweise als „Grund- oder Vertragsdaten"[462] bezeichnet. Der Gesetzgeber hat – anders als in § 15 Abs. 1 S. 2 TMG – absichtlich auf eine katalogartige Aufzählung möglicher Bestandsdaten verzichtet, um angesichts der Vielfältigkeit möglicher Telemediendienste eine flexible Qualifizierung von Daten als Bestandsdaten im Einzelfall zu ermöglichen.[463] § 14 Abs. 1 und 2 TMG stellen eine abschließende Regelung für die gesetzlich zulässige Verwendung von Bestandsdaten dar. Auf „andere Rechtsvorschriften" i.S.d. § 12 Abs. 1 TMG kann nicht zurückgegriffen werden, da nach dem Gesetzeszweck in solchen ein Zitiergebot beachtet werden müsste, also konkret auf Telemedien-Bestandsdaten Bezug genommen werden müsste. Solche Rechtsvorschriften wurden bisher nicht erlassen.[464] Eine über § 14 Abs. 1 und 2 TMG hinausgehende Verwendung von Bestandsdaten ist daher nur mit Einwilligung des Betroffenen zulässig (§ 12 Abs. 1 TMG).[465]

Klassische Bestandsdaten sind insbesondere: Personalien des Nutzers (Name und Anschrift, Email oder Telefonnummer), Log-In Daten (Nutzername und Passwort) und ggf. die IP-Adresse, Informationen über den verabredeten Abrechnungsmodus und konkrete Zahlungsmodalitäten.[466] Die Zulässigkeit der Datenverarbeitung durch den Diensteanbieter gemäß § 14 Abs. 1 TMG ist davon abhängig, welche dieser abstrakt als Bestandsdaten geeigneten Daten(-kategorien) im konkreten Fall für die Anbahnung, den Abschluss und die Durchführung des Telemedien-Nutzungsvertrags erforderlich sind.[467]

Die Legaldefinition in § 14 Abs. 1 TMG beschränkt den Adressatenkreis der Regelung auf jene Diensteanbieter (vgl. § 2 Nr. 1 TMG), die ihre Dienste dem Nutzer aufgrund eines Vertragsverhältnisses erbringen.[468] Maßgeblich ist hierfür nicht, ob der Diensteanbieter den Nutzern überhaupt einen Vertrag anbietet oder sogar „aufdrängt". Vielmehr muss die

---

462 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 12, m.w.N.; zustimmend *Hullen/Roggenkamp*, in: Plath, § 14 TMG, Rn. 9.
463 BT-Drs. 13/7385, S. 24; *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 13.
464 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 2.
465 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 2; *Hullen/Roggenkamp*, in: Plath, § 14 TMG, Rn. 8.
466 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 16; *Hullen/Roggenkamp*, in: Plath, § 14 TMG, Rn. 11.
467 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 15; *Hullen/Roggenkamp*, in: Plath, § 14 TMG, Rn. 12 ff.
468 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 9.

Erbringung des Telemediendienstes den Abschluss eines entsprechenden Vertrages voraussetzen oder ohne einen solchen zumindest mit schweren rechtlichen Nachteilen für den Diensteanbieter verbunden sein.[469] Dies wird unter anderem auch dann zu bejahen sein, wenn die Telemedien-Dienstleistung zwar unentgeltlich erbracht wird, der Diensteanbieter aber für ein rechtliches Fehlverhalten der Nutzer und hieraus resultierende Rechtsverletzungen Dritter zur Verantwortung gezogen werden könnte. Telemediendienste, bei denen ein Vertragsschluss von vorneherein nicht beabsichtigt wird und auch keine Rechtsverletzung Dritter durch andere Nutzer zu befürchten ist, zum Beispiel Nachrichten-, Wetter- oder andere Informationsportale[470], sind im Umkehrschluss aus dem Anwendungsbereich des § 14 TMG ausgeschlossen.

In sozialen Netzwerken hat der Anbieter ein legitimes Interesse, den Umgang der Nutzer untereinander durch allgemeine Nutzungsbedingungen zu regeln, um seine eigenen Haftungsrisiken wegen Rechtsverletzungen Dritter zu minimieren.[471] Die Einhaltung dieser Nutzungsbedingungen kann er sich von den Nutzern vertraglich zusichern lassen. Somit ist bei der Nutzung von sozialen Netzwerken regelmäßig vom Vorliegen eines Nutzungsvertrags über Telemedien-Dienstleistungen auszugehen. Für die Anwendbarkeit von § 14 Abs. 1 und 2 TMG kann es somit dahinstehen, ob die Nutzung von sozialen Netzwerken unentgeltlich erfolgt oder ob die Preisgabe von Nutzerdaten eine Art digitale Währung und somit eine Bezahlung darstellt[472], da in jedem Fall eine vertragliche Beziehung zugrunde liegt.

3. Nutzungsdaten

§ 15 Abs. 1 TMG definiert Nutzungsdaten als personenbezogene Daten eines Nutzers, die erforderlich sind, um die Inanspruchnahme des Dienstes zu ermöglichen und abzurechnen. § 15 TMG stellt für seinen Anwendungsbereich, ebenso wie § 14 TMG, eine abschließende Sonderregelung gegenüber den allgemeinen Regeln des BDSG sowie § 12 Abs. 1 TMG dar.[473]

---

469 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 10; *Hullen/Roggenkamp*, in: Plath, § 14 TMG, Rn. 2 ff.

470 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 10; vgl. auch *Hullen/Roggenkamp*, in: Plath, § 14 TMG, Rn. 4.

471 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 10, 36; *Hullen/Roggenkamp*, in: Plath, § 14 TMG, Rn. 4; zur Verantwortlichkeit des Anbieters sozialer Netzwerke für nutzergenerierte Inhalte noch ausführlich unten unter D.I.3.a).

472 Ausführlich zum ökonomischen Wert von Nutzerdaten: *Newman*, 40 William Mitchell L. Rev., 849 (860 ff.), 2013-2014; *Hoffmann-Riem*, Innovation und Recht, S. 630 ff.; vgl. auch *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 47; *Caspar*¸ ZD 2015, 12 (13); *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 80 f.; *Chmelik*, Social Network Sites, S. 79 ff. bejaht ausdrücklich die Qualität der zur Verfügung gestellten Nutzerdaten als entgeltliche Gegenleistung.

473 *Zscherpe*, in: Taeger/Gabel, § 15 TMG, Rn. 3.

Eine Abgrenzung zum TKG erfolgt gemäß § 11 Abs. 3 TMG nach einer inhaltlich-funktionellen Betrachtung, so dass Nutzungsdaten nach § 15 TMG vorliegen, sofern die Inhalte eines Dienstes im Vordergrund stehen, nicht eine bloße Übertragung von Informationen oder Signalen.[474] Anders als bei § 14 TMG ist das Vorliegen eines Vertragsverhältnisses zwischen dem Nutzer und dem Diensteanbieter nicht entscheidend.[475]

§ 15 Abs. 1 Nr. 1 TMG gibt katalogartige Beispiele für Nutzungsdaten, insbesondere Merkmale zur Identifikation des Nutzers, also Nutzer-ID, Passwort, Email-Adresse und ggf. die IP-Adresse sowie Angaben über Beginn, Ende und Umfang der Nutzung eines Telemediendienstes, welche vor allem in Cookies gespeichert werden. Gerade in Bezug auf Identifikationsdaten besteht also eine Überschneidung mit dem Anwendungsbereich des § 14 TMG. Ob die Daten als Bestandsdaten oder Nutzungsdaten zu behandeln sind, ist daher im Einzelfall nach dem jeweiligen Verwendungszweck zu beurteilen.[476]

Keine Nutzungsdaten sind Verbindungs- bzw. Verkehrsdaten, welche den §§ 95 ff. TKG unterfallen (dazu oben unter C.III.1). Auch Inhaltsdaten fallen nicht unter die Nutzungsdaten (dazu sogleich). Umstritten ist allerdings, wie die innerhalb des sozialen Netzwerks von Nutzern generierten Inhalte einzustufen sind. Während gelegentlich eine Einordnung als Nutzungsdaten vertreten wird, da sie „im Rahmen der Nutzung von Telemediendiensten anfallen“[477], handelt es sich richtigerweise um Inhaltsdaten. Der Streit wird im nächsten Abschnitt unter C.III.4.b) diskutiert.

Für den Erforderlichkeitsmaßstab des § 15 Abs. 1 TMG ist es ist notwendig, aber auch ausreichend, dass die „Inanspruchnahme des Telemediendienstes durch die Datenverarbeitung unmittelbar gefördert wird“, wobei auf das konkrete Nutzungsverhältnis abzustellen ist.[478] Schon vor Ende der Nutzung eines Dienstes im registrierten Bereich kann daher die Löschung bestimmer Daten wie etwa des Passworts geboten sein, wenn diese Daten nur in der Registrierungsphase bzw. der Phase des Einloggens erforderlich sind.[479]

Aus § 15 Abs. 1 TMG ergeben sich auch die maßgeblichen Grenzen für die Nutzung von Cookies. Im Rahmen dieser Arbeit erlangen Cookies vor allem im Rahmen der Reichweitenanalyse durch Facebook im Zusammenhang mit Social PlugIns, aber auch der

474 *Zscherpe*, in: Taeger/Gabel, § 15 TMG, Rn. 6.
475 *Zscherpe*, in: Taeger/Gabel, § 15 TMG, Rn. 10; *Spindler/Nink*, in: Spindler/Schuster, § 15 TMG, Rn. 2.
476 Vgl. *Spindler/Nink*, in: Spindler/Schuster, § 15 TMG, Rn. 2.
477 So *Zscherpe*, in: Taeger/Gabel, § 15 TMG, Rn. 28.
478 *Zscherpe*, in: Taeger/Gabel, § 15 TMG, Rn. 32; *Hullen/Roggenkamp*, in Plath, § 15 TMG, Rn. 15.
479 *Zscherpe*, in: Taeger/Gabel, § 15 TMG, Rn. 33; *Hullen/Roggenkamp*, in Plath, § 15 TMG, Rn. 16.

allgemeinen Nutzung von Facebook Relevanz. Inwieweit Facebooks Einsatz von Cookies rechtswidrig ist, insbesondere mit Blick auf den bereits beschriebenen datr-Cookie, soll unten unter D.I.3.c)aa)i) noch näher betrachtet werden.

4. Inhaltsdaten

Der Begriff der Inhaltsdaten wird weder im BDSG noch im TMG oder TKG erwähnt, wird aber von ihnen vorausgesetzt, da es neben Bestands-, Nutzungs- und Verkehrsdaten noch weitere Daten gibt. Obwohl dem Gesetzgeber das Fehlen einer entsprechenden Legaldefinition schon aus Diskussionen zum TDDSG bekannt war, hat er auf eine ausdrückliche Klarstellung im TMG verzichtet.[480] Als Inhaltsdaten werden in der Literatur ganz herrschend alle Daten bezeichnet, „die mit Hilfe eines Telemediendienstes übermittelt werden, um die durch den Teledienst begründeten Leistungs- und Rechtsverhältnisse zu erfüllen“[481]. Erfasst sind mithin solche Daten, die für die Nutzung des Telemediendienstes selbst nicht erforderlich sind, sondern lediglich vom Nutzer an den Anbieter übermittelt werden, um ein anderes Rechtsverhältnis, welches durch den Telemediendienst begründet wurde, erfüllen zu können. Dies betrifft insbesondere Lieferanschriften und konkrete Angaben über bestellte Waren beim Internetversandhandel oder online gebuchte (Reise-)Tickets.[482]

a) Anwendbarkeit des BDSG

Inhaltsdaten werden in der Literatur überwiegend als Datenart *sui generis* betrachtet, die nicht von den Regelungen des TMG erfasst sind, da sie nicht i.S.v. § 12 Abs. 1 TMG mit der Bereitstellung bzw. Erbringung des eigentlichen Telemediendienstes in Verbindung stehen und trotz langjähriger Diskussion nicht ausdrücklich von dem Gesetzgeber in die Regelungen des TMG aufgenommen wurden.[483] Die Zulässigkeit ihrer Verwendung richtet sich daher

---

480 Vgl. *Schmitz*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 16.2, Rn. 258; *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 20, dort in Fn. 36.

481 *Spindler/Nink*, in: Spindler/Schuster, § 15 TMG, Rn. 3; vgl. ebenfalls *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 19; *Redeker*, IT-Recht, Rn. 979 f.; *Hullen/Roggenkamp* in: Plath, § 14 TMG, Rn. 5; *Roßnagel*, in: ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 7.9, Rn. 59; *Engel-Flechsig*, Beck’scher IuKDG Kommentar § 5 TDDSG, Rn. 8.

482 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 19; *Redeker*, IT-Recht, Rn. 979; *Hullen/Roggenkamp*, in Plath, § 15 TMG, Rn. 12. Zur Einordnung von nutzergenerierten Inhaltsdaten in sozialen Netzwerken sogleich unten unter C.III.4.b).

483 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 20; *Redeker*, IT-Recht, Rn. 979; *Piltz*, Soziale Netzwerke, S. 68.

ausschließlich nach den Vorschriften des BDSG.[484] Eine Ausnahme hiervon soll nur dann gelten, wenn die Erbringung des durch den Telemediendienst begründeten Vertragsverhältnisses ihrerseits eine Telemediendienstleistung darstellt, da dies erneut den Anwendungsbereich des TMG eröffnen würde.[485]

b) Einordnung von nutzergenerierten Inhalten in sozialen Netzwerken

Umstritten ist dagegen die Behandlung der von Nutzern eingestellten Inhalte in sozialen Netzwerken. Während verbreitet eine Qualifikation als Inhaltsdaten befürwortet wird[486], wird zum Teil auch eine Qualifikation als Nutzungsdaten vertreten.[487] Die Zuordnung fällt nicht zuletzt deshalb so schwer, weil die möglichen Nutzungszwecke eines sozialen Netzwerk so vielfältig sind und entsprechend auch die zur Ermöglichung der Nutzung erforderlichen Daten im Sinne von § 15 TMG unterschiedlich bestimmt werden können. Von praktischer Relevanz ist die Einordnung insbesondere wegen der Erlaubnis des § 15 Abs. 3 TMG, wonach Nutzungsdaten zur pseudonymen Profilerstellung zu Werbe- und Marketingzwecken

---

484 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 20; *Redeker*, IT-Recht, Rn. 979; *Hullen/Roggenkamp*, in Plath, § 15 TMG, Rn. 12; *Piltz*, Soziale Netzwerke, S. 68; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 357; *Roßnagel*, in: ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 7.9, Rn. 59; *Kamp*, Personenbewertungsportale, S. 60 f.; *Arning/Moos*, ZD 2014, 126 (132); *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 94 f.; *Dies./Richter*, ZD 2012, 407 (409).

485 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 27. Eine differenziertere Ansicht (*Schmitz*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 16.2, Rn. 263 ff.) stuft die Inhaltsdaten zunächst als Nutzungsdaten i.S.v. § 15 Abs. 1 TMG ein, da sie im Rahmen der Nutzung des Telemediendienstes – etwa eines Online-Bestellservices – entstünden und auch erforderlich seien, um diesen Vorgang abzuschließen. Soweit das hierdurch begründete Vertragsverhältnis ebenfalls durch einen Telemediendienst abgewickelt werde, gelte weiterhin § 15 Abs. 1 TMG, etwa bei einer Download-Bestellung von Musikinhalten, welche elektronisch an den Nutzer übermittelt werden. Werde das weitere Vertragsverhältnis dagegen nicht durch einen Telemediendienst, sondern beispielsweise durch eine Zustellung per Post erbracht, unterliege die Datenverarbeitung den Vorschriften des BDSG. Die im Rahmen des Telemediendienstes erhobenen Daten dürften hierbei auch gemäß §§ 12 Abs. 1, 15 Abs. 1 TMG weiter verwendet werden, da sie für die Erbringung des Telemediendienstes in Form beispielsweise des „Bestelldienstes" nach § 15 Abs. 1 TMG erforderlich seien. Im Ergebnis bejaht also auch diese differenziertere Ansicht die Anwendbarkeit der Regelungen des BDSG auf Inhaltsdaten, sofern sie die Erbringung einer Leistung betreffen, die nicht ihrerseits durch Telemediendienste erfolgt. Diese Ansicht vermag aber nicht umfassend zu begründen, warum der Charakter der Daten sich nur durch eine Erfüllung des Vertrages mit einem anderen Medium ändern sollte. Überzeugender erscheint daher die h.M., wonach Daten, die für die Erfüllung eines mit Telemedien abgeschlossenen Vertrages erforderlich sind, generell als Inhaltsdaten einzustufen sind. Soweit es sich gleichzeitig um Nutzungsdaten handeln sollte, weil die vertragliche Leistung eine Telemediendienstleistung darstellt, sind gegebenenfalls kumulativ die Regelungen des § 15 TMG anzuwenden.

486 *Hullen/Roggenkamp*, in: Plath, § 15 TMG, Rn. 13; Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 14 f.; *Piltz*, Soziale Netzwerke, S. 68; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 357; *Dies.*, MMR 2011, 637 (639); Karg/*Fahl*, K&R 2011, S. 453 (458); *Redeker*, IT-Recht, Rn. 980; *Lerch/Krause/Hotho/Roßnagel*/*Stumme*, MMR 2010, S. 454 (546 f.); *Kamp*, Personenbewertungsportale, S. 61.

487 *Zscherpe*, in: Taeger/Gabel, § 15 TMG, Rn. 28; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 87; *ders./Nink*, in: Spindler/Schuster, § 15 TMG, Rn. 7 stufen die Daten zwar als Inhaltsdaten ein, wollen sie aber dennoch unter die Vorschrift des § 15 TMG subsumieren.

verwendet werden dürfen, solange der Nutzer nicht widerspricht. Bei Inhaltsdaten fehlt eine ausdrückliche gesetzliche Regelung zur Profilerstellung. Möchte man eine entsprechende Erlaubnis in § 28 Abs. 3 BDSG hinein lesen, so steht diese dennoch unter der deutlich engeren Voraussetzung, dass der Nutzer hierin aktiv eingewilligt haben muss.[488]

Soweit vertreten wird, dass die Daten als Nutzungsdaten anzusehen sind, weil sie „im Rahmen der Nutzung von Telemediendiensten anfallen“[489] oder eine „überragende[…] Bedeutung für die Nutzung der sozialen Netzwerke“ aufweisen[490], vermag dies nicht zu überzeugen: Eine derart weite Definition der Nutzungsdaten führte de facto dazu, dass sämtliche Daten im Rahmen von Telemediendiensten zunächst als Nutzungsdaten zu qualifizieren wären und die Regeln des § 15 TMG nur im Rahmen eines Spezialitätsverhältnisses gegenüber Bestands- und Verkehrsdaten zurücktreten würden. Zudem ist fraglich, ob bei von Nutzern bewusst ins soziale Netzwerk eingestellten Daten davon gesprochen werden kann, dass sie während der Telemediendienstnutzung „anfallen“. Eine undifferenzierte Betrachtungsweise übersieht hierbei, dass diese Daten gezielt anderen Nutzern zur Verfügung gestellt werden, während andere „typische“ Nutzungsdaten, wie Angaben über Beginn und Ende des Nutzungsvorgangs, IP-Adresse und Angaben über die aufgerufenen Seiten sowie die Verweildauer im Hintergrund von dem Anbieter gespeichert werden, ohne dass dies vom Nutzer beeinflusst werden kann.

Definiert man den Funktionszweck sozialer Netzwerke indes so weit, dass sie nicht nur der Kontaktpflege, sondern auch der neuen Kontaktakquise dienen, könnten gut ausgefüllte persönliche Profile durchaus den Status von für die Nutzung „erforderlichen“ Daten erhalten: Die Erbringung der Dienstleistung, einander zuvor fremde Menschen mit möglichst ähnlichen Interessen zusammenzuführen, kann nur dann erfolgsversprechend vollbracht werden, wenn möglichst viel über diese Personen bekannt ist. Soweit dies als integraler Bestandteil der Leistung des Telemediendienstes sozialer Netzwerke angesehen wird, könnten die Daten somit doch Nutzungsdaten im weitesten Sinne darstellen.[491]

Eine derartig weite Begriffsziehung würde aber die Abgrenzung zwischen den einzelnen Datenarten noch schwammiger werden lassen und damit sowohl erhebliche Rechtsunsicherheit kreieren als auch die Differenzierung letztlich obsolet machen. Dass von Nutzern eingestellte Inhalte in sozialen Netzwerken nicht vom Telos der Nutzungsdaten nach § 15 TMG erfasst

488 *Simitis*, in: Simitis, BDSG, § 28 Rn. 214.
489 *Zscherpe*, in: Taeger/Gabel, § 15 TMG, Rn. 28.
490 *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 87; vgl. auch *ders./Nink*, in: Spindler/Schuster, § 15 TMG, Rn. 7.
491 So *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 87.

sind, zeigt zudem § 15 Abs. 3 TMG, der eine Erstellung von pseudonymen Nutzungsprofilen zum Zwecke der Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien gestattet, eine Zusammenführung mit Identifizierungsdaten aber verbietet. In sozialen Netzwerken ist dies unmöglich. Die Einstellung von Inhaltsdaten dient der eigenen Profilerzeugung durch den Nutzer bzw. der Selbstdarstellung.[492] Indem der Nutzer Angaben zu seinen Vorlieben, Hobbies, Interessen und Charaktereigenschaften macht, will er sich seinen Freunden im sozialen Netzwerk präsentieren und ein bestimmtes Selbstbild erschaffen.[493] Ebendiese Daten werden vom Anbieter des sozialen Netzwerks aber auch genutzt, um Profile für Werbung und Ähnliches zu erstellen. Es wäre eine reine Fiktion, vom Netzwerkanbieter zu verlangen, die Daten einerseits zu speichern, um dem Nutzer die Selbstdarstellung zu ermöglichen, zu der er sich selbst entscheidet, den Anbieter aber gleichzeitig zu verpflichten, diese Daten nicht mit Identifizierungsdaten über den Nutzer in Verbindung zu bringen. Es ist daher insgesamt überzeugender, von Nutzern eingestellte Daten in sozialen Netzwerken als Inhaltsdaten und nicht als Nutzungsdaten zu betrachten. Die Zulässigkeit ihrer Erhebung, Speicherung und Verarbeitung richtet sich daher nach bisheriger nationaler Rechtslage nach dem BDSG.[494]

c) Begriff des personenbezogenen Datums

Das BDSG schützt gemäß § 1 Abs. 1 nur personenbezogene Daten. Hierbei handelt es sich gemäß der Legaldefinition in § 3 Abs. 1 BDSG, welche Art. 2 lit. d) DSRL umsetzt, um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Entscheidend ist also nicht unbedingt, dass das einzelne Datum bereits mit einer Person verknüpft ist, sondern es genügt, dass es mit einer Person verknüpft werden kann und somit personenbeziehbar ist. Die Personenbeziehbarkeit ist für jedes Datum neu zu prüfen. Sie ist zu bejahen, wenn eine Person objektiv identifiziert werden kann, also nach allgemeiner Lebenserfahrung und einem vernünftigerweise zu erwartenden Einsatz gegebenenfalls vorhandenen Zusatzwissens des Datenverarbeiters.

Probleme ergeben sich bei der Frage, welches Wissen Dritter für den Datenverarbeiter verfügbar ist und ihm zugerechnet werden muss bzw. ab wann von vollständig anonymisierten

---

492 *Grimmelmann*, 94 Iowa L.Rev. 1137 (1152 ff.), 2008-2009.

493 *Jandt/Roßnagel*, MMR 2011, 637 (637 f.).

494 So auch *Hullen/Roggenkamp*, in: Plath, § 15 TMG, Rn. 13; *Piltz*, Soziale Netzwerke, S. 68; Karg/*Fahl*, K&R 2011, S. 453 (458); *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 356 f.; *Dies./Ders.*, MMR 2011, 637 (639); *Redeker*, IT-Recht, Rn. 980; *Lerch/Krause/Hotho/Roßnagel/Stumme*, MMR 2010, S. 454 (546 f.); *Kamp*, Personenbewertungsportale, S. 58 ff.

Daten auszugehen ist. Die Frage wurde insbesondere im Zusammenhang damit diskutiert, ob dynamische IP-Adressen einen Personenbezug aufweisen. Anders als statische IP-Adressen sind dynamische IP-Adressen nicht einer Person fest zugeordnet, sondern werden bei jeder Anmeldung des Anschlusses neu vergeben.[495] Grundsätzlich verfügt somit nur der Access-Provider über die direkte Möglichkeit einer Zuordnung, während alle nachgeordneten Content-Provider auf sein Wissen zurückgreifen müssten, um die IP-Adresse einer konkreten Person zuzuordnen.[496]

Der BGH hatte die hochumstrittene Frage des Personenbezugs von dynamischen IP-Adressen dem EuGH zur Klärung vorgelegt.[497] Der EuGH hat daraufhin mit Urteil vom 19. Oktober 2016 entschieden, dass eine dynamische IP-Adresse für einen Diensteanbieter bzw. Content Provider ein personenbezogenes Datum darstellt, „wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.“[498] Die entsprechenden zur Verfügung stehenden rechtlichen Mittel legt der EuGH dabei sehr weit aus, da es explizit ausreichen soll, wenn eine Bestimmung der Person mit Hilfe Dritter, wie etwa der zuständigen Behörde oder eben dem Internetzugangsanbieter unter den gesetzlichen Voraussetzungen möglich ist, da diese Mittel „vernünftigerweise eingesetzt werden könnten“.[499] Hiervon ausgehend wertet nunmehr auch der BGH dynamische IP-Adressen als personenbezogene Daten i.S.v. § 12 Abs. 1 TMG i.V.m. § 3 Abs. 1 BDSG.[500]

Diese höchstrichtliche Rechtsprechung stellt einen vermittelnden Weg zwischen den zuvor vertretenen Begriffen der relativen und absoluten Bestimmbarkeit dar. Sie folgt im Prinzip – wenngleich nicht explizit – dem Begründungsansatz des relativen Bestimmbarkeitsbegriffs, indem sie auf das Kriterium der vernünftigerweise zu erwartenden Zugriffsmöglichkeit auf das Wissen Dritter abstellt.[501] Da die Rechtsprechung die vernünftigerweise zu erwartenden Mittel aber denkbar weit auslegt und das Vorhandensein abstrakter rechtlicher Möglichkeiten, die

---

495 Ausführlich: *Nietsch*, Anonymität, S. 74 ff.; *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, S. 376.

496 *Nietsch*, Anonymität, S. 77; *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, S. 380 ff.

497 BGH, ZD 2015, 80 (80 ff.); vgl. im Übrigen auch die sehr vertiefte Darstellung bei *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, S. 268 ff. 286 ff., 372 ff.

498 EuGH, *Breyer*, Rs. C-582/14, Rn. 49 = NJW 2016, 3579 (3581).

499 EuGH, *Breyer*, Rs. C-582/14, Rn. 47 = NJW 2016, 3579 (3581).

500 BGH, ZD 2017, 424 (426).

501 Instruktiv zum relativen Bestimmbarkeitsbegriff: *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 342 ff.; *Dammann*, in: Simitis, BDSG, § 3 Rn. 26, 32; *Eßer*, in: Auernhammer, § 3 BDSG, Rn. 19; Schreibauer, in: Auernhammer, § 11 TMG Rn. 10; *Gola/Schomerus*, § 3 BDSG, Rn. 10, 44; vgl. insbesondere auch die sehr ausführliche Diskussion bei *Nietsch*, Anonymität, S. 92 ff.

unter strengen Voraussetzungen stehen, ausreichen lässt, sind die praktischen Auswirkungen eher mit denen des absoluten Bestimmbarkeitsbegriffs vergleichbar. Dieser stellt darauf ab, ob irgendeine Person mit dem entsprechenden Zusatzwissen die IP-Adresse einem Betroffenen zuordnen könnte.[502]

Mit den ergangenen Entscheidungen dürfte der Streit nunmehr grundsätzlich für die Praxis entschieden sein, wobei aber zu erwarten steht, dass der genaue Umfang der „vernünftigerweise zu erwartenden Mittel" weiterhin Gegenstand gerichtlicher Auseinandersetzungen sein wird.

Für die Anbieter sozialer Netzwerke war und ist der Streit nur von untergeordneter Bedeutung, da diese in aller Regel selbst über notwendiges Zusatzwissen verfügen, um sogar eine dynamische IP-Adresse einer Person zuzuordnen. Dies gilt insbesondere dann, wenn bei der Anmeldung zwingend der bürgerliche Name und weitere persönliche Daten wie das Geburtsdatum oder der Wohnort angegeben werden müssen.[503] Nur soweit eine vollständig anonyme Nutzung des sozialen Netzwerks ermöglicht wird, wäre eine Personenbeziehbarkeit fraglich. Selbst dann ist eine Zuordnung allerdings über Trackingmöglichkeiten wie das Browser-Fingerprinting oder auch Cookies grundsätzlich möglich, so dass prinzipiell alle im Rahmen der Nutzung des sozialen Netzwerks anfallenden Daten für den Anbieter des sozialen Netzwerks als personenbezogen einzustufen sind.[504]

---

502 *Weichert*, in: DKWW, § 3 BDSG, Rn. 13; vgl. auch *Schild*, in: Wolff/Brink, § 3 BDSG, Rn. 97; *Pahlen-Brandt*, K&R 2008, 288 (289) m.w.N.

503 *Schreibauer*, in: Auernhammer, § 11 TMG Rn. 9; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 344; *Karg/Thomsen*, DuD 2012, 729 (734); zur Rechtmäßigkeit dieses sogenannten Klarnamenzwangs angesichts der Regelung in § 13 Abs. 6 TMG vgl. unten unter D.II.2.

504 Vgl. *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 72 f.; *Nietsch*, Anonymität, S. 76 f.; *Karg/Thomsen*, DuD 2012, 729 (734).

D. Regulatorische Probleme sozialer Netzwerke

Soziale Netzwerke offenbaren besonders deutlich die Verschiebung, die das Akteursgeflecht datenschutzrechtlicher Beziehungen in den letzten Jahrzehnten durchlaufen hat. Zu Beginn der Datenschutzgesetzgebung in den 1970er und 80er Jahren war regelmäßig von einem zwei-Personen-Verhältnis zwischen Datenverarbeiter und Betroffenem auszugehen, häufig lag zudem eine Staat-Bürger Beziehung vor. In sozialen Netzwerken agieren dagegen vor allem Private untereinander. Hierbei gibt es zahlreiche Beteiligte, insbesondere andere Nutzer, Werbetreibende, Verwender von Social-PlugIns, sowie Anbieter von Apps und sonstigen Dienstleistungen. Der Staat ist unmittelbar nur insoweit involviert, als er als Nutzer oder Ermittlungsbehörde in strafrechtlichen oder nachrichtendienstlichen Angelegenheiten an dem sozialen Netzwerk partizipiert.[505] Im Folgenden soll untersucht werden, ob die geltenden Datenschutzgesetze sich als flexibel genug für diese veränderten Bedingungen erweisen oder ob „eine grundsätzliche Neukonzeption des Datenschutzrechts erforderlich ist“[506]. In diesem Zusammenhang wird ebenfalls untersucht, ob und ggf. inwieweit die DS-GVO eine Verbesserung und Lösung der Probleme darstellt oder diese letztlich perpetuiert.

Nachdem im vorigen Kapitel der datenschutzrechtliche Rahmen sozialer Netzwerke sowohl nach bisheriger als auch zukünftiger Rechtslage bestimmt wurde, rückt nun unter D.I. die Frage ins Zentrum der Betrachtung, inwieweit das vom zwei-Personen-Verhältnis her gedachte Datenschutzrecht im Rahmen des Konzepts des „Verantwortlichen“ für eine Datenverarbeitung mit den mehrseitigen Rechtsbeziehungen in sozialen Netzwerken umgehen kann. Die informationelle Selbstbestimmung der Nutzer wirkt dabei allenfalls mittelbar zwischen den Beteiligten, ist also nur im Rahmen einer staatlichen Schutzpflicht von rechtspraktischer Bedeutung.[507]

Das an verschiedenen Stellen im Internet auftretende Spannungsverhältnis zwischen Anonymität und einer effektiven Rechtsdurchsetzung tritt auch in sozialen Netzwerken auf und

---

505 Der hierin liegende Wandel von einer nur bipolaren Rechtsbeziehung hin zu einem multipolaren Rechtgeflecht betrifft mitnichten nur das Datenschutzrecht sozialer Netzwerke, sondern stellt eine grundsätzliche Herausforderung an das Verwaltungsrecht dar; hierzu bereits vertieft *Hoffmann-Riem*, Rechtsformen, Handlungsformen, Bewirkungsformen, in: in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II, § 33, Rn. 40 ff.

506 So *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 387; vgl. auch *Schneider/Härting*, ZD 2011, 63 (64); *Buchholtz*, AöR 2015, 121 (123); *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 27.

507 *Greve*, Drittwirkung, in: FS Kloepfer, S. 671 ff.; zur informationellen Selbstbestimmung noch ausführlicher unten unter D.III.4.a).

kristallisiert sich dort insbesondere in den Fragen der Impressums- und Klarnamenspflicht, auf welche vertieft unter D.II. eingegangen werden soll.

Das dritte hier im Fokus stehende Problem stellt der regulatorische Umgang mit dem Informations- und Machtgefälle dar, das regelmäßig in sozialen Netzwerken zwischen Nutzern, Regulierern, Betreiben und sonstigen Akteuren besteht. Hierbei sind insbesondere Fragen an die Steuerungsfähigkeit des Rechts und die Leistungsfähigkeit der Einwilligung zu stellen. Diesen Fragen soll unter D.III. nachgegangen und mögliche Lösungsansätze diskutiert werden.

I. Komplexe Rechtsbeziehungen vs. ein klassisch dichotomes Datenschutzrecht: Das Problem der Verantwortlichkeit

Eine Beurteilung der Effektivität des Datenschutzrechts in Bezug auf soziale Netzwerke bedarf einer Analyse, inwieweit das bisherige und zukünftige Datenschutzrecht auf die in den sozialen Netzwerken vertretenen Akteure überhaupt anwendbar ist bzw. in welchem Umfang es ihnen Pflichten auferlegt. Zentral ist hierfür der Begriff des „Verantwortlichen", an den sowohl im nationalen, als auch im europäischen Datenschutzrecht die datenschutzrechtlichen Pflichten geknüpft werden.[508] Im vorigen Kapitel wurden kollisionsrechtliche Aspekte dieser Frage erörtert, vor allem mit Blick auf unterschiedliche Niederlassungen. Im Folgenden soll es dagegen um die materiell-rechtliche Verantwortungszuweisung an die Akteure in sozialen Netzwerken gehen.

1. Akteure in sozialen Netzwerken

Soziale Netzwerke stellen ein mehrseitiges Rechtsverhältnis mit zahlreichen Akteuren dar. Das klassische dichotome Verhältnis zwischen dem Anbieter und dem individuellen Nutzer als „Betroffenem" der Datenverarbeitung wird zunächst um dritte Nutzer erweitert, die mit dem Betroffenen interagieren und auf seine Daten zugreifen sowie Daten über ihn verbreiten können.[509] Die Gruppe der Nutzer ist hierbei sehr breit gefächert und erfasst einerseits Verbraucher, die ein persönliches Profil pflegen und in vielen Fällen noch minderjährig sind.[510] Andererseits umfasst sie auch wirtschaftliche Akteure, die in Form von „Fanpages" oder

508 *Dammann*, in: Simitis, BDSG, § 3 Rn. 224; *Wedde*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 4.3, Rn. 1; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 376.

509 Vgl. auch bereits *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 129.

510 Nach einer Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) sind Minderjährige nicht nur bei Facebook angemeldet, sondern nutzen dies sogar teils sehr intensiv; so gaben 36% der befragten und bei Facebook angemeldeten 9-13-Jährigen an, das soziale Netzwerk täglich zu nutzen, unter den 14-17-Jährigen betrug dieser Anteil sogar 68%, *DIVSI*, U25-Studie v. Februar 2014, S. 69 f.

Ähnlichem Werbung für sich und ihre Produkte oder Dienstleistungen machen und das soziale Netzwerk als Kommunikationsplattform mit Kunden und Interessenten nutzen.[511] Im Rahmen modernerer und benutzerfreundlicher Kommunikationsstrategien greift auch der Staat immer wieder auf Facebook Fanseiten zurück, um mit den Bürgern in Kontakt zu treten.[512] Zudem kann es sich bei Fanseiten um (quasi-)journalistische Angebote handeln, die durch die Verknüpfung von Blogs und vergleichbaren Seiten mit einem Social-Media Account die Reichweite und Verbreitung ihres Angebots steigern. Hierbei handelt es sich um einen Sonderfall der wirtschaftlichen Nutzung der Profile sozialer Netzwerke mit einem besonderen Schwerpunkt auf der Verbreitung von Nachrichten und Informationen, bei dem über presserechtliche Privilegierungen nachgedacht werden kann.[513]

Unmittelbar mit dem sozialen Netzwerk verknüpft, wenngleich nicht zwingend in ihm selbst als Nutzer vertreten, gibt es sodann die Social PlugIn-Verwender und Werbekunden des Anbieters. Letztere kaufen vom Anbieter des sozialen Netzwerks (anonymisierte) Nutzerprofile, um den entsprechenden – durch Cookies zuzuordnenden – Nutzern anschließend zielgerichtete, personalisierte Werbung im Internet anzeigen zu können.[514] Ein prominentes Beispiel für Social Plug-Ins ist der sogenannte „Like-Button“ von Facebook, der mittlerweile auf zahlreichen Webseiten im Internet eingebunden ist.[515]

Eine letzte Kategorie bilden nichtangemeldete Personen, deren Daten gleichsam als „Kollateralschäden“ den Anbietern sozialer Netzwerke zugänglich gemacht werden, indem angemeldete Nutzer Informationen über sie posten oder dem Anbieter Emailadressbücher zur Verfügung stellen (z.B. durch den „Freundefinder“ bei Facebook[516]). Im Rahmen des Besuchs von Facebook-Fanpages und Webseiten mit Social-PlugIns fallen sie zudem unter eine Reichweitenanalyse, indem sie beispielsweise im Falle von Facebook durch den datr-Cookie identifizierbar und im Internet verfolgbar werden.[517]

---

511 *Pießkalla*, ZUM 2014, S. 368 (370); *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (2 f.); *Lichtnecker*, GRUR 2013, 135 (136).

512 *Caspar*, ZD 2015, 12 (12 f.); *Martini/Fritzsche*, VerwArch (104) 2013, 449 (450); ausführlich zu Fanpages der öffentlichen Hand unten unter D.I.3.c)dd).

513 Art. 29 DatSchGruppe, Stellungnahme 5/2009, WP 163, S. 7; vgl. auch *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 349, dort Fn. 35.

514 Hierzu oben unter B.II.3.b)bb)ii).

515 Hierzu ausführlich oben unter B.II.2.b)aa).

516 Vgl. oben unter B.II.3.b)aa)i).

517 Vgl. zu Tracking-Methoden oben unter B.II.2.b); allgemein zu den Problemen im Umgang mit Kollateraldaten im Datenschutzrecht: *Cebulla*, ZD 2015, 507 ff.

Ob und ggf. wieweit diese Akteure datenschutzrechtlichen Pflichten unterliegen, ist davon abhängig, inwiefern sie unter den zentralen Begriff des „Verantwortlichen" subsumiert werden können. Speziell bei datenverarbeitenden Nutzern stellt sich zudem die Frage, ob das Datenschutzrecht überhaupt anwendbar ist oder das sogenannte „Haushaltsprivileg" nach § 1 Abs. 2 Nr. 3 BDSG bzw. Art. 2 Abs. 2 lit. c) DS-GVO greift.

2. Das Konzept der Verantwortlichkeit im Datenschutzrecht

Der Begriff der „verantwortlichen Stelle" stellt den zentralen Anknüpfungspunkt für datenschutzrechtliche Bestimmungen und Pflichten dar.[518] Die DS-GVO übernimmt in Art. 4 Nr. 7 wortgleich die bisherige Definition des Art. 2 lit. d) DSRL, so dass auch unter ihrer Geltung die hier zu diskutierenden Probleme fortbestehen werden.[519]

§ 3 Abs. 7 BDSG als bisher maßgebliche nationale Norm verfolgt einen primär handlungsorientierten Definitionsansatz, der Datenverarbeitung in Form von Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung erfasst. In europarechtskonformer Auslegung ist das flexiblere und der heute vorherrschenden Arbeitsteilung angemessenere Merkmal der Entscheidungsbefugnis über Zwecke und Mittel der Datenverarbeitung (Art. 2 lit. d) DSRL), welches zukünftig nach Art. 4 Nr. 7 DS-GVO allein maßgeblich sein wird, allerdings bereits heute hineinzulesen.[520] Dieses flexiblere Merkmal lässt sich zudem indirekt aus der Verantwortung für die Datenverarbeitung des Auftragsdatenverarbeiters gemäß § 3 Abs. 7 letzter Hs. BDSG ableiten. Der grundsätzliche datenschutzrechtliche Verantwortlichkeitsbegriff bleibt daher durch die Einführung der DS-GVO unverändert.

Im TMG und TKG findet der Begriff der „verantwortlichen Stelle für die Datenverarbeitung" keine Verwendung. Stattdessen wird dort grundsätzlich auf den Diensteanbieter (§ 2 Nr. 1 und 2 TMG) abgestellt bzw. auf die Person oder das Unternehmen, die bzw. das geschäftsmäßig TK-Dienste erbringt oder an ihrer Erbringung mitwirkt (§ 91 i.V.m. § 3 TKG). Diensteanbieter im Sinne des § 2 Nr. 1 TMG ist, wer eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt. Nicht erforderlich ist, dass der Anbieter auch

---

518 *Dammann*, in: Simitis, BDSG, § 3 Rn. 1 f., 224; *Schild*, in: Wolff/Brink, § 3 BDSG, Rn. 110; *Eßer*, in: Auernhammer, § 3 BDSG, Rn. 70; *Wedde*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 4.3, Rn. 1; zur kollisionsrechtlichen Bedeutung schon ausführlich oben unter C.II.4.

519 So auch bereits *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (16); vgl. auch *Faust/Spittka/Wybitul*, ZD 2016, 120 (122 f.).

520 Hierzu bereits oben unter C.II.4.a).

Eigentümer der hierfür notwendigen Infrastruktur, also beispielsweise der Server und Anschlüsse, ist, solange diese Kapazitäten überhaupt vorhanden sind und der Anbieter zumindest zeitweise über diese bestimmen kann.[521] Gemäß § 12 Abs. 3 TMG sind allerdings, soweit nichts anderes bestimmt ist, die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden. Daher ist insbesondere auf § 3 Abs. 7 BDSG zurückzugreifen, wenn es um die Ermittlung der datenschutzrechtlichen Verantwortlichkeit eines Diensteanbieters geht.[522]

Die Verantwortlichkeit ist immer in Bezug auf eine konkrete Datenverarbeitung zu bestimmen, also nicht absolut an feste Rollen gebunden.[523] Allerdings geht das Gesetz dabei von einer eindeutigen Zuweisbarkeit von Verantwortung für einzelne Verarbeitungsvorgänge aus. In der von mehrpoligen Verhältnissen und Arbeitsteilung geprägten Realität im Internet stößt dieses Konzept schnell an Grenzen.[524] Outsourcing und Arbeitsteilung zwischen unterschiedlichen Unternehmen, ebenso wie die gemeinsame Autorenschaft verschiedener Datenverarbeiter beispielsweise an Big Data Ergebnissen führen gleichsam zu einer Verantwortungsdiffusion, die eine genaue Zuordnung erschwert.[525] Auch in Bezug auf Cloudspeicherdienste kommt es zu erheblichen Abgrenzungsschwierigkeiten.[526] Konkret in sozialen Netzwerken stellt das unter 3. zu analysierende komplexe Akteursgeflecht eine große Herausforderung für die Bestimmung der datenschutzrechtlichen Verantwortlichkeit dar.

---

521 OLG Düsseldorf, K&R 2013, S. 594 (597); OLG Düsseldorf, MMR 2013, S. 718 (718); OLG Düsseldorf, MMR 2008, S. 682 (683); *Roßnagel*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 7.9, Rn. 47; *Ricke*, in: Spindler/Schuster, § 2 Rn. 2; *Sieber/Höfinger*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 18.1., Rn. 30 f.; *Lorenz*, VuR 2014, S. 83 (86); *Richter*, MMR 2014, S. 517 (518).

522 *Gerhold*, ZIS 2015, 156 (159); *Moos*, in: Taeger/Gabel, § 11 Rn. 28; *Schulz/Hoffmann*, in: PdK, Band L 16 Bund, Rn. 87; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 16; vgl. auch *Spindler/Nink*, in: Spindler/Schuster, § 12 TMG, Rn. 8; *Kamp*, Personenbewertungsportale, S. 37 ff., 50.

523 Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 10.

524 *Spindler*, GRUR-Beilage 2014, S. 101 (104); *Dammann*, in: Simitis, BDSG, § 3 Rn. 2, 20 f.; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 376; vgl. auch *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 27.

525 Ausführlich *Dammann*, in: Simitis, BDSG, § 3 Rn. 2; *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 32 f.

526 Instruktiv: *Maisch*, Informationelle Selbstbestimmung, S. 119 ff.; *Kroschwald*, ZD 2013, 388 (389 ff.); *Wagner/Blaufuß*, BB 2012, 1751 ff.; *Schulz*, MMR 2010, 75 (78 f.); *Pohle/Ammann*, CR 2009, 273 (276 f.); *Niemann/Paul*, K&R 2009, 444 (448 f.); vgl. auch Art. 29 DatSchGruppe, Stellungnahme 5/2012, WP 196, S. 6 ff.; *Dammann*, in: Simitis, BDSG, § 3 Rn. 2.

a) Auftragsdatenverarbeitung

Eine gewisse Form der gesetzlichen Aufspaltung der Verantwortlichkeit stellt die Auftragsdatenverarbeitung gemäß § 11 BDSG bzw. Art. 17 Abs. 2 und 3 DSRL und zukünftig Art. 28 DS-GVO dar. Sie ist die einzige Konstellation, in der sich das Gesetz explizit mit dem Auseinanderfallen von konkretem Datenverarbeiter und dem für die Datenverarbeitung Verantwortlichen beschäftigt. Die DS-GVO nimmt dabei keine wesentlichen Änderungen an den Anforderungen vor, die auch bereits nach dem BDSG bestanden.[527]

Bei einer Auftragsdatenverarbeitung verbleibt die Verantwortlichkeit bei dem Auftraggeber, vgl. §§ 11 Abs. 1, 3 Abs. 7 BDSG, sowie zukünftig *e contrario* Art. 28 Abs. 10 DS-GVO.[528] Der Auftraggeber muss den Auftragsdatenverarbeiter sorgfältig aussuchen und einen schriftlichen, detaillierten Auftrag erteilen, in dem neben dem Umfang und Zweck der Datenverarbeitung insbesondere auch die technischen und organisatorischen Maßnahmen gemäß § 9 BDSG zur Umsetzung der sich aus dem BDSG ergebenden Pflichten spezifiziert sind (§ 11 Abs. 2 Nr. 3 BDSG bzw. zukünftig Art. 28 Abs. 1 DS-GVO). Sodann hat der Auftraggeber den Auftragsdatenverarbeiter regelmäßig zu kontrollieren, um sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Der Auftragsdatenverarbeiter wiederum unterliegt einem strikten Weisungsrecht des Auftraggebers. Soweit er der Ansicht ist, dass eine Weisung gegen Datenschutzbestimmungen verstößt, hat er ihn darauf unverzüglich hinzuweisen (§ 11 Abs. 3 BDSG bzw. Art. 28 Abs. 3 S. 3 DS-GVO). Die Eigenschaft als Auftragsdatenverarbeiter ist immer in einem spezifischen Kontext und bezogen auf konkrete Tätigkeiten zu ermitteln, sie folgt nicht bereits daraus, dass es sich um eine datenverarbeitende Organisation handelt.[529] Die Konsequenz einer wirksamen Auftragsdatenverarbeitung ist, dass die Beteiligten zueinander nicht als Dritte anzusehen sind, vgl. § 3 Abs. 8 S. 3 BDSG bzw. Art. 4 Nr. 10 DS-GVO; sie werden vielmehr als rechtliche Einheit aufgefasst, so dass Datenweitergaben nicht als Übermittlungen i.S.v. § 3 Abs. 4 BDSG anzusehen sind und entsprechend ohne eine gesetzliche Erlaubnis oder die Einwilligung der

---

527 Ausführlich *Hofmann*, in: Roßnagel, (Hrsg.), Europäische DS-GVO, § 3 Rn. 250 ff.; vgl. auch *Gierschmann*, ZD 2016, 51 (52).

528 *Eßer*, in: Auernhammer, § 3 BDSG, Rn. 75; *Petri*, in: Simitis, BDSG, § 11 Rn. 1, 22, 48; *Spoerr*, in: Wolff/Brink, § 11 BDSG, Rn. 34; *Plath/Schreiber*, in: Plath, § 3 BDSG, Rn. 71. Art. 28 Abs. 10 DS-GVO stellt allerdings klar, dass dem Auftragnehmer eine eigene Verantwortlichkeit zukommt, sofern er entgegen der Regelungen der Verordnung selbst über die Zwecke und Mittel der Datenverarbeitung bestimmt. Dies betont auch § 62 BDSG Abs. 7 n.F. gemäß Art. 1 DSAnpUG-EU, freilich nur im Rahmen des Anwendungsbereichs der Vorschrift, welcher sich nach § 45 BDSG n.F. bestimmt und insbesondere im Hinblick auf die hier diskutierten Pflichten Privater in sozialen Netzwerken nicht besteht.

529 Art. 29 DatSchGruppe, Stellungnahme 1/2010, WP 169, S. 30; vgl. auch *Petri*, in: Simitis, BDSG, § 11 Rn. 22 ff.

Betroffenen erfolgen dürfen.[530] Diese mitunter als „Privilegierung der Auftragsdatenverarbeitung“[531] bezeichnete vereinfachte Möglichkeit der Datenweitergabe wird allerdings kompensiert durch die strengen formalen Anforderungen an das Auftragsverhältnis.[532]

Die vollständige Verantwortung und Kontrollpflicht des Auftraggebers wirkt auf den ersten Blick in einer analogen Welt verankert, in denen die Daten in Papierform oder auf Festplatten vor Ort verfügbar waren, so dass der Auftraggeber sich regelmäßig persönlich von der ordnungsgemäßen Aufbewahrung der Daten überzeugen konnte.[533] In einer Welt von global verteilten und vernetzten Servern und Rechenzentren wirkt dies in vielen Fällen nur als eine Fiktion, wenn nicht gar eine unmöglich umsetzbare Pflicht.[534] Einen Ausweg bietet hier indes die Möglichkeit, die eigenhändige Überprüfung vor Ort durch aussagekräftige Datenschutzzertifizierungen oder -audits des Auftragnehmers zu ersetzen.[535] Diesen Weg eröffnet zukünftig auch explizit Art. 28 Abs. 5 DS-GVO.

Für soziale Netzwerke erlangt die Frage der Auftragsdatenverarbeitung nach Ansicht mancher Autoren insbesondere im Zusammenhang mit der datenschutzrechtlichen Verantwortlichkeit von Fanpage-Betreibern Relevanz.[536] Hierauf soll unten unter D.I.3.c)bb) ausführlich eingegangen werden.

b) Gemeinsame Verantwortlichkeit vs. faktische Verantwortungsdiffusion

§ 3 Abs. 7 BDSG schließt – trotz der konsequenten Verwendung des Singulars – nicht aus, dass mehrere juristische oder natürliche Personen für den Umgang mit personenbezogenen Daten

---

530 *Petri*, ZD 2015, 305 (306); *Plath*, in: Plath, § 11 BDSG, Rn. 2; *Gabel*, in: Taeger/Gabel, § 11 BDSG, Rn. 2; *Spoerr*, in: Wolff/Brink, § 11 BDSG, Rn. 4; *Thomale*, in: Auernhammer, § 11 BDSG, Rn. 3; *Wedde*, in: DKWW, § 11 BDSG, Rn. 18.

531 *Koós/Englisch*, ZD 2014, 276 (277); *Roßnagel/Kroschwald*, ZD 2014, 495 (497); vgl. auch *Plath*, in: Plath, § 11 BDSG, Rn. 4.

532 Vereinzelt wird in Frage gestellt, ob diese automatische Privilegierung der Auftragsdatenverarbeitung unter Geltung der DS-GVO aufrechterhalten bleibt (so etwa *Petri*, ZD 2015, 305 (308 f.)) oder die Datenweitergabe zukünftig über eine Interessenabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO zu legitimieren ist (so *Roßnagel/Kroschwald*, ZD 2014, 495 (497)). Einen Mittelweg beschreiten hierbei *Koós/Englisch*, ZD 2014, 276 (284 f.), die zwar die Anwendbarkeit des Art. 6 Abs. 1 lit. f) DS-GVO bejahen, aber scheinbar eine Vermutung zugunsten der Zulässigkeit der Übermittlung aufstellen wollen, was eine „tatsächliche Privilegierung“ begründen würde. Da diese Frage für die hier diskutierten Probleme nicht von entscheidender Relevanz ist, soll auf sie nicht vertieft eingegangen werden.

533 Vgl. *Petri*, in: Simitis, BDSG, § 11 Rn. 59; *Plath*, in: Plath, § 11 BDSG, Rn. 5.

534 *Plath*, in: Plath, § 11 BDSG, Rn. 4 f.; *Koós/Englisch*, ZD 2014, 276 (279).

535 *Petri*, in: Simitis, BDSG, § 11 Rn. 59; *Thomale*, in: Auernhammer, § 11 BDSG, Rn. 37, 43.

536 Vgl. z.B. ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 17 f.

gemeinsam verantwortlich sind.[537] Art. 2 lit. d) DSRL und Art. 4 Nr. 7 DS-GVO verweisen ausdrücklich darauf, dass die Entscheidung über die Zwecke und Mittel der Verarbeitung „allein oder gemeinsam" getroffen werden kann.

Als problematisch erweisen sich indes Fälle, in denen eine eindeutige Zuordnung der Verantwortlichkeit zu einem Datenverarbeiter faktisch als nicht möglich oder zumindest sehr schwierig erweist.[538] Einige Autoren wollen bei derartiger arbeitsteiliger Datenverarbeitung die Begriffe der „kollektiven" und „kumulativen" Verantwortlichkeit einführen, um eine nuanciertere Beurteilung der Verantwortlichkeit zu ermöglichen. Eine kollektive Verantwortlichkeit soll vorliegen, wenn die „beteiligten Akteure arbeitsteilig für bestimmte Daten und bestimmte Phasen des Datenumgangs verantwortlich sind".[539] Die einzelnen Verantwortungsbereiche sollen in diesem Fall nebeneinander, sich nicht überschneidend bestehen.[540] Effektiv erfolgt damit eine vollständige Verantwortungszuweisung an eine Stelle und eine Aufspaltung großer, zusammenhängender Datenverarbeitungsprozesse in sehr kleinteilige Datenverarbeitungsschritte, die vermeintlich unabhängig voneinander sind. Eine kumulative Verantwortlichkeit umfasse dagegen die „volle Verantwortlichkeit beider oder aller beteiligten Stellen für alle Daten und alle Phasen des Datenumgangs".[541]

Jandt und *Roßnagel* ist sicherlich in der Problemanalyse zuzustimmen, dass eine eindeutige Zuordnung von Verantwortlichkeit in sozialen Netzwerken durch die Aufspaltung in zahlreiche Datenverarbeitungsvorgänge unterschiedlicher Akteure mit ungleicher technischer Beherrschung schwierig ist.[542] Die vorgeschlagene Trennung nach einzelnen Arbeitsschritten und einer hieraus resultierenden vollständigen Verantwortungszuweisung funktioniert

---

537 *Dammann*, in: Simitis, BDSG, § 3 Rn. 226; *Weichert*, in: DKWW, § 3 BDSG, Rn. 57; *Eßer*, in: Auernhammer, § 3 BDSG, Rn. 76; *Spoerr*, in: Wolff/Brink, § 11 BDSG, Rn. 60; *Plath/Schreiber*, in: Plath, § 3 BDSG, Rn. 69; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 348; *Kamp*, Personenbewertungsportale, S. 43 ff.

538 Vgl. *Spiecker gen. Döhmann*, Verantwortung bei begrenztem Wissen, in: Fehling u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 65 ff. – *Erscheinen in Vorbereitung*; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 376; *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 32; *Petri*, ZD 2015, 103 (106); *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 135 f.; *Martini/Fritzsche*, VerwArch (104) 2013, 449 (462 f.).

539 *Jandt/Roßnagel*, ZD 2011, 160 (161), die sich in ihrer Analyse vor allem mit der jeweiligen Verantwortlichkeit des Anbieters und der Nutzer für nutzergenerierte Inhalte auseinandersetzen; vgl. auch *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 361; zustimmend: *Kroschwald*, ZD 2013, 388 (389).

540 *Jandt/Roßnagel*, ZD 2011, 160 (161).

541 *Jandt/Roßnagel*, ZD 2011, 160 (161).

542 *Jandt/Roßnagel*, ZD 2011, 160 (161).

allerdings nur in Konstellationen, in denen keine Verantwortungsdiffusion vorliegt.[543] Soweit zur Bestimmung einer kollektiven Verantwortlichkeit ein eigentlich arbeitsteiliger Verarbeitungsschritt einem einzelnen Akteur vollständig zugerechnet wird, handelt es sich dagegen im Ergebnis um eine Fiktion nach dem klassischen dichtomen Muster von Verarbeiter und Betroffenem, nicht aber eine Auflösung der Verantwortungsdiffusion. Sie kann insbesondere im Kontext sozialer Netzwerke zur unbilligen Enthaftung von Akteuren führen, die arbeitsteilig an einem Datenverarbeitungsprozess partizipieren und diesen maßgeblich mitgestalten, aber weniger unmittelbaren Einfluss hierauf haben als ein anderer Akteur.[544]

Das geltende Datenschutzrecht kennt keinen teilweise Verantwortlichen.[545] Dies ist folgerichtig im Rahmen des Datenschutzrechts als besonderem Ordnungsrecht. Es ist zwar möglich, dass der individuelle Pflichtenumfang variiert oder nur eine subsidiäre Inanspruchnahme im Rahmen der ordnungsrechtlichen Störerauswahl in Betracht kommt.[546] Die Stellung als ordnungsrechtlicher Verantwortlicher an sich liegt indessen zwingend ganz oder gar nicht vor. Die datenschutzrechtliche Verantwortlichkeit als Anknüpfungspunkt für Rechte und Pflichten[547] ist somit logisch in ihrem Grundbestand nicht teilbar.

Diese Unteilbarkeit der Verantwortlichkeit ist angesichts der durch Arbeitsteilung und Verantwortungsdiffusion bestimmten Praxis der Datenverarbeitung ein Problem, das indes durch Anerkennung einer kumulativen Verantwortlichkeit auf Rechtsfolgenseite gelöst wird: Wenn mehrere Beteiligte gemeinsam über die Zwecke und Mittel einer Datenverarbeitung entscheiden, aber nach außen unklar ist, von wem exakt welcher Beitrag ausgeht, so haften sie nach außen gleichsam in einer Gesamtschuld.[548] Die Rechtsfolge ist, dass die einschlägigen Betroffenenrechte gegen jeden der Verantwortlichen geltend gemacht werden können. Ebenso können ordnungsrechtliche Verfügungen gegen jeden der kumulativ Verantwortlichen gerichtet

---

543 Wie zuvor unter C.II.4. beschrieben, ist bei der Bestimmung der Verantwortlichkeit stets nach der Kontrolle über die Mittel und Zwecke einer konkreten Datenverarbeitung zu fragen, so dass eine Trennung nach einzelnen Arbeitsschritten grundsätzlich immer vorgenommen wird. Ein Anwendungsbereich für die differenziertere kollektive vs. kumulative Verantwortlichkeit ergibt sich folglich nur in Konstellationen, in denen es bei der Verantwortlichkeitszuweisung nach diesem Maßstab zu Problemen kommt.

544 Hierzu ausführlich sogleich unter D.I.3 und insbesondere D.I.3.a)aa).

545 Vgl. *Weichert*, in: DKWW, § 3 BDSG, Rn. 62; *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (10 f.).

546 Für eine derart abgestufte Verantwortlichkeit plädieren beispielsweise *Petri*, ZD 2015, 103 (106); *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 135 f.; vgl. auch Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 14.

547 *Dammann*, in: Simitis, BDSG, § 3 Rn. 1 f., 224; *Wedde*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 4.3, Rn. 1.

548 *Dammann*, in: Simitis, BDSG, § 3 Rn. 226; Art. 29 DatSchGruppe, Stellungnahme 1/2010, WP 169, S. 30; vgl. auch *Weichert*, in: DKWW, § 3 BDSG, Rn. 62.

werden.[549] Die kumulative Verantwortlichkeit auf Rechtsfolgenseite überwindet folglich die tatbestandliche Fiktion der kollektiven Verantwortlichkeit und betrachtet arbeitsteilige Datenverarbeitungsprozesse in ihrem jeweiligen Kontext.

Diesen Weg beschreitet auch Art. 26 DS-GVO: Im Falle der gemeinsamen Festlegung der Zwecke und Mittel der Datenverarbeitung müssen die verschiedenen Verarbeiter eine für den Betroffenen transparente Vereinbarung treffen, wem von ihnen welche Verantwortlichkeiten und entsprechend auch Pflichten zukommen. Ungeachtet dieser internen Festlegungen haften sie gegenüber dem Betroffenen nach außen gemäß Art. 26 Abs. 3 DS-GVO als Gesamtschuldner. § 63 BDSG n.F. gemäß Art. 1 DSAnpUG-EU enthält eine mit Art. 26 DS-GVO vergleichbare Bestimmung, ist aber gemäß § 45 BDSG n.F. nur auf die Datenverarbeitung durch öffentliche Stellen zu Zwecken gemäß Art. 1 Abs. 1 der Richtlinie (EU) 2016/680[550], also insbesondere der Verhütung, Ermittlung und Verfolgung von Straftaten oder Ordnungswidrigkeiten anwendbar. Außerhalb dieses Bereichs gilt der Anwendungsvorrang der DS-GVO, wie auch § 1 Abs. 5 BDSG n.F. deklaratorisch feststellt.

Die Regelung des Art. 26 DS-GVO erweist sich als sachgerecht und wirkt der Verantwortungsdiffusion effektiv entgegen. Ein wirksamer Schutz der informationellen Selbstbestimmung der Betroffenen ist nicht möglich, wenn die Verantwortlichkeit durch intransparente Gestaltungen bis zur Unkenntlichkeit verschleiert wird.[551] Das Recht braucht letztendlich einen klaren Adressaten, da Betroffene nur dann ihre Rechte durchsetzen können, wenn klar ist, an wen sie oder der Staat sich wenden müssen. Zwar muss diesem Ansatz kritisch entgegen gehalten werden, dass er nur eine Regelung auf Rechtsfolgenseite darstellt, aber nicht dazu beiträgt, auch auf tatbestandlicher Ebene eine eindeutige Bestimmung der individuellen Verantwortlichkeit im klassischen dichtomen Sinne zu ermöglichen.[552] Die Abgrenzungsprobleme, wann eine hinreichende Mitbestimmung über die Zwecke und Mittel der Verarbeitung vorliegen, werden hierdurch nicht gelöst. Trotzdem ist die Regelung zu begrüßen, da sie zumindest die Rechtsdurchsetzung in Zweifelsfällen für den Betroffenen

549 *Dammann*, in: Simitis, BDSG, § 3 Rn. 226; *Spoerr*, in: Wolff/Brink, § 11 BDSG, Rn. 63; vgl. auch *Faust/Spittka/Wybitul*, ZD 2016, 120 (123).

550 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

551 *Dammann*, in: Simitis, BDSG, § 3 Rn. 226; *Klar*, DÖV 2013, 103 (109); Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 11; Art. 29 DatSchGruppe, Stellungnahme 1/2010, WP 169, S. 29; vgl. auch *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 136.

552 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (16).

erleichtert und das Risiko intransparenter Verarbeitungsstrukturen auf die Datenverarbeiter verlagert.[553]

Selbst wenn sich die technische und tatsächliche Datenverarbeitung also in Richtung einer vollständigen Auflösung von individuellen Verantwortungsstrukturen entwickeln sollte, erweist sich das Recht durch die Figur der kumulativen Verantwortlichkeit mit der Rechtsfolge einer Gesamtschuld als fähig, hiermit umzugehen. Eine weitere Abgrenzung zu einer „kollektiven Verantwortlichkeit" scheint demgegenüber wenig zusätzliche Rechtssicherheit und -klarheit zu bringen.

Im Ergebnis ist somit immer nach unterschiedlichen Datenverarbeitungsschritten zu differenzieren und individuell zu untersuchen, welcher Akteur die Kontrolle im Sinne der verantwortlichen Stelle hat und entsprechend als Verantwortlicher einzustufen ist.[554] Soweit sich dies tatbestandlich aufgrund einer faktischen Verantwortungsdiffusion nicht abschließend klären lässt, sind die Beteiligten auf Rechtsfolgenseite als kumulativ Verantwortliche zu behandeln. Was dies für die Verantwortlichkeit der Akteure in sozialen Netzwerken bedeutet, soll im Folgenden analysiert werden.

3. Datenschutzrechtliche Verantwortlichkeit der Akteure in sozialen Netzwerken im Einzelnen

Im multipolaren Geflecht sozialer Netzwerke stellt sich die Frage, inwieweit die unterschiedlichen Akteure jeweils als datenschutzrechtlich Verantwortliche zu klassifizieren sind. Besondere Probleme bereiten hierbei Nutzer, die Daten über Betroffene verwenden und verarbeiten, die Betreiber von Fanpages und die Verwender Social-PlugIns. Obwohl es sich um praktisch überaus relevante Problemstellungen handelt und die Fragen nach der grundsätzlichen

---

553 Letztendlich ist die Kompensation der Verantwortungsdiffusion auf Tatbestandsseite durch die Zuweisung einer kumulativen Verantwortlichkeit auf Rechtsfolgenseite nachgerade eine unabdingbare Konsequenz einer immer stärkeren arbeitsteiligen Datenverarbeitung: Wo es keinen einzelnen Akteur mehr gibt, der für einen einzelnen Datenverarbeitungsschritt alleine verantwortlich gemacht werden kann – also alleine über die Zwecke und Mittel der Datenverarbeitung bestimmt –, dort kann das Recht einen solchen auch nicht identifizieren. Die Verantwortlichkeit dennoch nur einem einzelnen Akteur aufzuerlegen, würde regelmäßig zu unbilligen Enthaftungen anderer Akteure führen, die ebenfalls an der Datenverarbeitung partizipieren und von ihr profitieren und zudem eine Zurechnung fremder Verantwortlichkeit für den einzelnen Akteur bedeuten.

554 So auch *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 135 f.; *Petri*, ZD 2015, 103 (106); *Plath/Schreiber*, in: Plath, § 3 BDSG, Rn. 69; *Dammann*, in: Simitis, BDSG, § 3 Rn. 224 ff.; vgl. zum hierfür maßgeblichen funktionellen Begriff der Verantwortlichkeit bereits oben unter C.II.4.

datenschutzrechtlichen Verantwortlichkeit durchaus nicht einfach zu beantworten sind, werden sie bisher nur vereinzelt vertieft diskutiert.[555]

Wie zuvor bereits beschrieben wurde, bietet die DS-GVO keine grundlegenden Neuerungen bei der allgemeinen Verantwortungszuweisung, sondern übernimmt den bisherigen europäischen Verantwortlichkeitsbegriff wortgleich in Art. 4 Abs. 5. Gegenüber der bisherigen Rechtslage findet allerdings eine erhebliche Reduzierung der Erlaubnistatbestände statt, die mit Recht als „unterkomplex" bezeichnet wurde.[556] Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten wird sich zukünftig an Art. 6 DS-GVO messen lassen müssen. Hiernach ist eine Datenverarbeitung insbesondere aufgrund einer wirksamen Einwilligung zulässig (Art. 6 Abs. 1 lit. a) DS-GVO) oder wenn sie notwendig ist, um einen Vertrag durchführen zu können (Art. 6 Abs. 1 lit. b) DS-GVO). Hervorzuheben ist zudem der Auffangtatbestand des Art. 6 Abs. 1 lit. f) DS-GVO, wonach die Verarbeitung zulässig ist, wenn das Interesse des Verarbeiters oder eines Dritten an der Verarbeitung die berechtigten Interessen, Grundrechte oder Grundfreiheiten des Betroffenen überwiegen.[557] Gemäß Art. 13 Abs. 1 lit. c) DS-GVO sind die verfolgten berechtigten Interessen des Datenverarbeiters oder des Dritten gegenüber dem Betroffenen offen zu legen.

Zwar entspricht die Formulierung des Art. 6 DS-GVO weitgehend dem bisherigen Art. 7 DSRL, so dass auf europäischer Ebene im ersten Zugriff keine großen Änderungen erfolgen. Durch die unmittelbare Anwendbarkeit entfallen aber die bisherigen mitgliedstaatlichen Befugnisse zur Konkretisierung, soweit diese trotz der umfassend harmonisierenden Wirkung der DSRL zulässig waren.[558] In Deutschland betrifft dies in Bezug auf soziale Netzwerke insbesondere die Regelungen der §§ 11 ff. TMG, sowie die sehr differenziert ausgestalteten Erlaubnistatbestände der §§ 28, 29 BDSG. Die DS-GVO statuiert damit einen in ihrem Erwägungsgrund 15 explizit formulierten Regelungsansatz der Technologieneutralität, der dem vom Bundesverfassungsgericht einst im Volkszählungsurteil angemahnten bereichsspezifischen Regelungsansatz diametral entgegensteht.[559] Es liegt auf der Hand, dass

---

555 Vgl. auch schon *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 346; wichtige Analysen leistet insoweit bereits *Piltz*, Soziale Netzwerke, S. 87 ff., 183 ff., fokussiert sich dabei allerdings – getreu dem zivilrechtlichen Schwerpunkt seiner Arbeit – auf einige Einzelfragen.

556 So *Roßnagel/Nebel/Richter*, ZD 2015, 455 (460); *ders./dies./ders.*, ZD 2013, 103 (104); kritisch auch *Schmitz*, in: Hoeren/Sieber/Holznagel, Teil 16.2, Rn. 37; *Sydow/Kring*, ZD 2014, 271 (272 f.); *Herrmann*, ZD 2014, 439 (440); *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 129; *Nebel/Richter*, ZD 2012, 407 (409 f.).

557 Zum Umfang der kollisionsrechtlichen und materiellen Anwendbarkeit der DS-GVO bereits oben unter C.I.

558 Hierzu bereits ausführlich oben unter C.II.2.

559 BVerfGE 65, 1 (46) – Volkszählung; so auch bereits *Nebel/Richter*, ZD 2012, 407 (407).

derart vage Formulierungen, wie sie die DS-GVO in diesem Kontext aufweist, bei ihrer direkten Anwendung zu erheblicher Rechtsunsicherheit führen und langwieriger gerichtlicher Klärung bedürfen werden.[560] Speziell für Datenverarbeiter bedeutet dies erhebliche ökonomische Risiken und Planungsunsicherheiten, während Betroffene Schwierigkeiten bei der Durchsetzung ihrer Rechte haben könnten.

Mit Anwendbarkeit der DS-GVO wird sich die Einstufung als Diensteanbieter gemäß § 2 Nr. 1 u. 2 TMG für die Bestimmung der datenschutzrechtlichen Pflichten erübrigen, soweit die §§ 11 ff. TMG durch die Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO verdrängt werden und es nur noch auf die Stellung als verantwortliche Stelle gemäß Art. 4 Nr. 7 DS-GVO ankommt. Auch die aktuell noch vorzunehmende Abgrenzung von Bestands-, Nutzungs- und Inhaltsdaten wird dann entfallen.[561] Hiermit entfallen aber auch die bisher mit der Einteilung einhergehende Zweckbindung bei der Verarbeitung und der demokratisch ausgehandelte gesetzliche Interessenausgleich.[562] Eine wissenschaftliche Analyse, wie eine Gewichtung der Interessen im Einzelfall konkret vorzunehmen ist, ist auf einem derart hohen Abstraktionslevel, wie es Art. 6 DS-GVO vorgibt, wenig erkenntnisversprechend und läuft Gefahr, der Beliebigkeit anheim zu fallen. Entsprechende Probleme werden sich aber ohne jeden Zweifel auch in der Rechtspraxis ab der Anwendbarkeit der DS-GVO stellen.

Wie oben unter C.I.2. ausgeführt wurde, ist es nicht ausgeschlossen – allerdings angesichts des vollharmonisierenden Anspruchs der DS-GVO unwahrscheinlich –, dass die Regelungen des §§ 11 ff. TMG als bereichsspezifische Konkretisierungen i.S.v. Erwägungsgrund 10 DS-GVO anwendbar bleiben. Auch ohne eine solche nationale Konkretisierbarkeit der DS-GVO spricht aber Vieles dafür, die dort getroffenen Abwägungen jedenfalls faktisch im Rahmen der nach Art. 6 Abs. 1 lit. f) DS-GVO vorzunehmenden Interessenabwägung beizubehalten, um zugunsten der Rechtssicherheit Fallgruppen zu bilden und dogmatische Ordnung zu schaffen. Dieser Ansatz bietet sich auch zur Systematisierung der für einen Vertragsschluss notwendigen Daten gemäß Art. 6 Abs. 1 lit. b) DS-GVO an.

---

560 *Roßnagel*, in: Ders. (Hrsg.), Europäische DS-GVO, § 1 Rn. 39 f.; *Ders./Nebel/Richter*, ZD 2015, 455 (457); *Sydow/Kring*, ZD 2014, 271 (272 f.); *Gierschmann*, ZD 2016, 51 (55); *Keppeler*, MMR 2015, 779 (782), der allerdings zugleich das Entfallen von Abgrenzungsschwierigkeiten begrüßt; ausführlich zum Regelungsansatz der Technologieneutralität noch unten unter E.I.1.

561 Ausführlich: *Geminn/Richter*, in: Roßnagel (Hrsg.), Europäische DS-GVO, § 4 Rn. 291 ff.; *Nebel/Richter*, ZD 2012, 407 (409); *Keppeler*, MMR 2015, 779 (780 ff.); vgl. auch *Schmitz*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 16.2, Rn. 36; zu dieser Abgrenzung bereits oben unter C.III.

562 *Nebel/Richter*, ZD 2012, 407 (409).

Dabei ist natürlich zu beachten, dass mitgliedstaatliche Normen nicht zur Bestimmung des Anwendungsbereichs und Inhalts einer europäischen Verordnung herangezogen werden können, sondern gleichsam eine niedrigere Stellung in der Normenhierarchie einnehmen.[563] Dies gilt umso mehr im Zusammenhang mit einer Verordnung wie der DS-GVO, die ausweislich ihres Erwägungsgrundes 10 eine vollharmonisierte Regelung anstrebt.[564] Der einheitliche Vollzug einer Verordnung innerhalb der Mitgliedstaaten wäre durch mitgliedstaatliche Konkretisierungen gefährdet, so dass eine Unabhängigkeit der Verordnungsanwendung von mitgliedstaatlichen Regelungen auch aus dem Grundsatz des *effet utile* folgt.

Gleichzeitig darf aber nicht übersehen werden, dass die DS-GVO trotz ihres explizit vollharmonisierenden Anspruchs fast 50 Öffnungsklauseln für mitgliedstaatliche Regelungen enthält.[565] Neben den vagen Formulierungen insbesondere in den Erlaubnistatbeständen ist sie daher in manchen Teilen ohne weitere Konkretisierung schlicht nicht vollzugsfähig.[566] *Kühling* und *Martini* gehen daher sogar so weit, die DS-GVO als eine „Richtlinie im Verordnungsgewand"[567] bzw. ein faktisch „atypische[s] Hybrid aus Verordnung und Richtlinie"[568] zu bezeichnen. Jedenfalls eine dogmatische Konkretisierung der Vorschriften erscheint daher geboten, um Rechtssicherheit und -klarheit zu schaffen.

Insbesondere die Regelungen der §§ 14, 15 TMG und §§ 28, 29 BDSG stellen zudem europarechtskonforme Konkretisierungen des mit Art. 6 DS-GVO weitgehend inhaltsgleichen, vollharmonisierenden Art. 7 DSRL dar.[569] Es ist der DS-GVO nicht zu entnehmen, dass sie eine grundsätzlich andere Gewichtung und Abwägung der Interessen vornehmen wollte als dies unter der DSRL noch der Fall war.[570] Wenngleich Art. 6 DS-GVO also nicht formal durch die nationalen Normen konkretisiert werden kann, so können diese nationalen Normen doch im Rahmen der historischen Auslegung wertvolle Anhaltspunkte dafür bieten, wie der Wille des europäischen Gesetzgebers bisher und durch die geringen Änderungen damit auch zukünftig zu interpretieren ist.

---

563 *Haratsch/Koenig/Pechstein*, Europarecht, Rn. 179 ff., 382 f.
564 Vgl. zum umfassenden Harmonisierungsanspruch der DS-GVO *Klar*, DÖV 2013, 103 (111 f.).
565 *Kühling/Martini*, EuZW 2016, 448 (448).
566 So ausdrücklich auch *Kühling/Martini*, EuZW 2016, 448 (449); sehr kritisch auch *Roßnagel*, in: Ders. (Hrsg.), Europäische DS-GVO, § 1 Rn. 43 ff.
567 *Kühling/Martini*, EuZW 2016, 448 (448).
568 *Kühling/Martini*, EuZW 2016, 448 (449).
569 Vgl. bereits für die Vorgängerregelungen der §§ 5, 6 TDDSG zu §§ 14, 15 TMG ausführlich *Schulz*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, § 1 TDDSG, Rn. 21, § 5 TDDSG, Rn. 20, § 6 TDDSG Rn. 16.
570 So auch *Schantz*, NJW 2016, 1841 (1841).

Daher soll die folgende Analyse der Verantwortlichkeit der einzelnen Akteure in sozialen Netzwerken vornehmlich anhand der bisher anwendbaren nationalen Normen durchgeführt werden, inklusive der sich aktuell stellenden Abgrenzungsprobleme, die sich durch die maximal vereinheitlichende Norm des Art. 6 Abs. 1 DS-GVO formal erübrigen werden. Gegenüber einer Interessenabwägung im weitgehend rechtsfreien, unbestimmten Raum bietet dies den dogmatischeren und rechtssicheren Zugriff, dessen Erkenntnisse für die Auslegung der zukünftigen Rechtslage genutzt werden können.

a) Verantwortlichkeit der Anbieter sozialer Netzwerke

Die Anbieter sozialer Netzwerke ermöglichen die Nutzung dieser Dienstleistung und halten diese in Form von Telemedien bereit. Ihr Angebot stellt sich auch für einen objektiven Dritten als eigenständiger Internetauftritt dar. Sie sind daher als Diensteanbieter im Sinne von § 2 Nr. 1 und 2 TMG bzw. § 91 i.V.m. § 3 TKG einzustufen und somit Adressaten der telemedienrechtlichen Datenschutzvorschriften der §§ 12 ff. TMG, soweit der Umgang mit Bestands- und Nutzungsdaten betroffen ist.[571] Sie entscheiden über die Art, Dauer und Notwendigkeit der Speicherung zu Zwecken der Nutzungsermöglichung des Dienstes, die Nutzung der Daten im Rahmen von Werbung und Analyseverfahren und, durch die Gestaltungsmacht über die AGB, über Zwecke und Mittel der Datenverarbeitung. Es ist dabei unerheblich, ob sie ihr Diensteangebot auf eigenen oder (teilweise) fremden Servern ablegen.[572] Mit der Anwendbarkeit der DS-GVO erübrigt sich gegebenenfalls ihre Einstufung als Diensteanbieter, soweit es nur noch auf ihre Stellung als verantwortliche Stelle nach Art. 4 Nr. 7 DS-GVO und die Rechtmäßigkeit der Datenverarbeitung nach Art. 6 Abs. 1 DS-GVO ankommt.

aa) Verantwortlichkeit für von Nutzern generierte Inhaltsdaten

Anbieter sozialer Netzwerke verarbeiten zahlreiche Arten von Daten über ihre Nutzer.[573] Eine vollständige Analyse der Rechtmäßigkeit würde den Rahmen dieser Arbeit sprengen und muss

---

571 *Kremer*, RDV 2014, 73 (74); *Polenz*, VuR 2012, 207 (211); *Piltz*, Soziale Netzwerke, S. 105 f.; *Piltz/Trinkl*, in: Hoeren/Bensinger, Kap. 13, Rn. 15 und 147 ff.; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 356 f.; *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 92; zur Unterscheidung von Bestands-, Nutzungs- und Inhaltsdaten vgl. schon oben unter C.III.

572 OLG Düsseldorf, K&R 2013, S. 594 (597); OLG Düsseldorf, MMR 2013, S. 718 (718); OLG Düsseldorf, MMR 2008, S. 682 (683); *Roßnagel*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 7.9, Rn. 47; *Holznagel/Ricke*, in: Spindler/Schuster, § 2 Rn. 2; *Lorenz*, VuR 2014, S. 83 (86); *Richter*, MMR 2014, S. 517 (518).

573 Vgl. bereits den Überblick oben unter B.II.2.

einem Praxiskommentar sowie der Rechtsprechung vorbehalten bleiben.[574] Daher soll hier nur das besonders strittige Problem der datenschutzrechtlichen Verantwortlichkeit für die Verarbeitung von nutzergenerierten Inhaltsdaten aufgegriffen werden, insbesondere wenn es sich bei diesen um personenbezogene Daten über Dritte handelt.

Maßgeblich war bisher § 3 Abs. 7 BDSG, da das TMG keine eigenen Regelungen über die datenschutzrechtliche Verantwortlichkeit aufweist, mithin gemäß § 12 Abs. 3 TMG subsidiär auf die Regelungen des BDSG zurückzugreifen ist.[575] Zudem unterfallen Inhaltsdaten nach vorzugswürdiger Ansicht nicht dem TMG als Nutzungsdaten, sondern als Datenart *sui generis* dem BDSG.[576] Da Art. 4 Nr. 7 DS-GVO den bisherigen Verantwortlichkeitsbegriff der DSRL unverändert übernimmt, erübrigt sich zukünftig allenfalls diese Abgrenzung, aber es ergeben sich keine weiteren inhaltlichen Änderungen.

Bei der Klärung der Verantwortlichkeit ist nach unterschiedlichen Verarbeitungsschritten zu differenzieren. Soweit die Anbieter die von Nutzern übermittelten Inhaltsdaten für Werbezwecke analysieren und an Dritte weitergeben, sind dies unzweifelhaft Datenverarbeitungsschritte, für die sie auch verantwortlich sind.[577] Problematisch ist aber, ob die Anbieter auch unabhängig von einer späteren Verarbeitung konkreter Inhaltsdaten bereits für die bloße Übermittlung dieser Daten durch die Nutzer und die anschließende Speicherung und Verbreitung verantwortlich sind.[578] Die Klärung der Anbieterverantwortlichkeit für die Übermittlung von Inhaltsdaten durch die Nutzer ist insofern von großer praktischer Bedeutung, als die genaue Verarbeitung von Daten zu Werbezwecken durch die Anbieter sehr intransparent für Außenstehende ist. Wäre also eine aktive Weiterverarbeitung durch den Anbieter maßgeblich, wäre es im Einzelfall schwierig nachzuweisen, für welche Verarbeitung von Inhaltsdaten die Anbieter genau verantwortlich sind. Zudem wäre natürlich auch der Datenverarbeitungsvorgang unterschiedlich, für den eine gesetzliche Erlaubnis oder eine Einwilligung des Betroffenen vorliegen müsste. Dies beträfe nämlich entweder die grundsätzliche Übermittlung aller Inhaltsdaten durch die Nutzer an den Anbieter und die

---

574 Eine ausführliche Analyse der zivilrechtlichen Verantwortlichkeit und Haftung der Anbieter sozialer Netzwerke leistet bereits *Chmelik*, Social Network Sites, S. 67 ff.

575 *Gerhold*, ZIS 2015, 156 (159); *Moos*, in: Taeger/Gabel, § 11 Rn. 28; *Schulz/Hoffmann*, in: PdK, Band L 16 Bund, Rn. 87; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 16; vgl. auch *Spindler/Nink*, in: Spindler/Schuster, § 12 TMG, Rn. 8; *Kamp*, Personenbewertungsportale, S. 37 ff., 50.

576 Hierzu ausführlich oben unter C.III.4.

577 *Jandt/Roßnagel*, ZD 2011, 160 (161); *Dies./Ders.*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 356 ff.; Art. 29 DatSchGruppe, Stellungnahme 5/2009, WP 163, S. 6.

578 *Peifer*, K&R 2011, 543 (545) weist zutreffend daraufhin, dass die „Veröffentlichung von Daten" nicht von § 4 Abs. 1 BDSG umfasst wird, lässt aber offen, ob die hierfür erforderlichen Verarbeitungsvorgänge erfasst sind und zu einer datenschutzrechtlichen Verantwortlichkeit von Anbietern sozialer Netzwerke führen.

Zugänglichmachung im Nutzerprofil oder aber die Analyse der Inhaltsdaten durch den Anbieter und die Weitergabe spezifischer, gegebenenfalls sogar bereits pseudonymisierter Inhaltsdaten zu Werbezwecken an Dritte.

Aus praktischer Sicht ist die Frage der Anbieterverantwortlichkeit vor allem für die Erhebung und Speicherung von nutzergenerierten Inhaltsdaten über Dritte relevant. Von der Antwort hängt beispielsweise ab, ob Betroffene datenschutzrechtliche Auskunfts- und Löschungsrechte direkt gegen den Anbieter des sozialen Netzwerks geltend machen können oder sich stets an den anderen Nutzer verweisen lassen müssen, der die Daten übermittelt hat. Zudem müsste der Anbieter durch einen gesetzlichen Erlaubnistatbestand oder eine Einwilligung des Betroffenen legitimiert sein, wenn es sich um eine gesonderte Form der Datenverarbeitung handelt, für die er die datenschutzrechtliche Verantwortung trägt.

Bei nutzergenerierten Inhalten über die eigene Person ist die Frage dagegen weit weniger dringlich, da in aller Regel eine Einwilligung des übermittelnden Nutzers in die Speicherung und Übermittlung der Daten anzunehmen ist bzw. keine Anhaltspunkte für ein entgegenstehendes Interesse im Sinne der §§ 28 Abs. 1 S. 1 Nr. 2, 29 Abs. 1 Nr. 1 BDSG bzw. zukünftig Art. 6 Abs. 1 lit. f) DS-GVO vorliegen.[579] Während dem Anbieter des sozialen Netzwerks also auch bei diesen Daten eine Verantwortlichkeit für die Erhebung und Speicherung der Daten zukommen kann, wird dies regelmäßig aufgrund der maßgeblichen Mitwirkung der Betroffenen und der damit ausgedrückten Einwilligung nicht zu praktischen Problemen führen. Deutlich problematischer kann sich dies freilich für über die bloße Speicherung und Übermittlung hinausgehende Verarbeitungen darstellen, wenn der Anbieter die Daten zur Profilerstellung für Werbezwecke oder Ähnlichem verwendet.[580]

Unstreitig haben die Anbieter die maßgeblichen Einflussmöglichkeiten auf die technischen Aspekte der Speicherung und Übermittlung der Inhaltsdaten. Zudem entscheiden sie allein über die Mittel der Datenverarbeitung, indem sie den Code und die Algorithmen der Datenverarbeitung bereitstellen. Es wird aber vertreten, dass dem Anbieter für die bloße Bereitstellung dieser Inhaltsdaten durch die Nutzer keine Verantwortlichkeit zukomme, da er diese weder selbst erheben würde, noch über die konkreten *Zwecke* entscheiden könnte, aus denen diese Daten übermittelt und gespeichert würden.[581] Vielmehr liege diese Auswahl allein

---

579 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 358 f.; vgl. auch *Spindler/Nink*, in: Spindler/Schuster, § 4a BDSG Rn. 17.

580 Zu den hierbei auftretenden Problemen bei der Einwilligung ausführlich unten unter D.III.2.b).

581 *Jandt/Roßnagel*, ZD 2011, 160 (161); vgl. auch *Kroschwald*, ZD 2013, 388 (389).

im Ermessen der Nutzer, die hierbei ein individuelles Selbstdarstellungs- und Kommunikationsinteresse verfolgten. Die bloße faktische Möglichkeit des Anbieters, bestimmte Datenübermittlungen zu unterbinden, genüge nicht, um seine Verantwortlichkeit zu begründen, zumal ein solcher Eingriff der Zwecksetzung zuwiderlaufe, Nutzer zur Generierung von Inhaltsdaten zu verleiten.[582] *Jandt* und *Roßnagel* wollen hierbei nach der oben beschriebenen kollektiven und kumulativen Verantwortlichkeit unterscheiden. Im Ergebnis plädieren sie für eine kollektive, sich also nicht überschneidende Verantwortlichkeit, soweit die Nutzer in Ausnutzung ihrer vom Anbieter eingeräumten Handlungsfreiheiten selbstständig über die Auswahl und den Zweck der übermittelten Inhaltsdaten entscheiden.[583] Zwar soll es sich bei jeder Einstellung von Daten durch die Nutzer für den Plattformanbieter gleichzeitig um eine Erhebung von Daten im Sinne von § 3 Abs. 3 BDSG handeln, für die dieser entsprechend verantwortlich sei. Eine konkrete Abfrage einzelner Informationen sei nicht erforderlich, solange der allgemeine Zweck der Plattform sei, dass Nutzer Informationen für Dritte bereitstellten.[584] Zudem speichere er die Daten gemäß § 3 Abs. 4 Nr. 1 BDSG, um eine Abfrage der Daten durch andere Nutzer zu ermöglichen.[585] Trotzdem seien die Anbieter im Rahmen der gestuften kollektiven Verantwortlichkeit dann nicht verantwortlich, wenn sie die gemäß §§ 28 Abs. 1 S. 1 Nr. 2, 29 Abs. 1 Nr. 1 BDSG erforderliche Interessenabwägung in Bezug auf ein einzelnes Datum nicht vornehmen könnten, also insbesondere dann, wenn es um die Veröffentlichung von personenbezogenen Daten Dritter gehe. Einerseits sei die Menge der Nutzereinträge zu groß für eine solche individuelle Prüfung, andererseits könne der Anbieter den Wahrheitsgehalt der Aussagen nicht überprüfen.[586] Das Datenschutzrecht könne aber nur solche Pflichten an einen Verantwortlichen stellen, die dieser auch tatsächlich erfüllen kann. Insofern seien die Nutzer primär für die Einhaltung der datenschutzrechtlichen Regelungen

582 *Jandt/Roßnagel*, ZD 2011, 160 (161).

583 So noch *Jandt/Roßnagel*, ZD 2011, 160 (161); etwas zurückhaltender *Dies./Ders.*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 348: Durch die „Festlegung des thematischen Kontexts und die verschiedenen Funktionen" werde die Entscheidung des Zwecks durch den Anbieter „vorgegeben oder zumindest beeinflusst". Somit sei der Anbieter voll verantwortlich, gegebenenfalls kumulativ mit den Nutzern, wenn eine eindeutige Zuordnung der Verantwortlichkeit nicht möglich sei. Dies soll indes dann wieder nicht gelten, wenn der Anbieter die Rechtmäßigkeit der Übermittlung der Daten nicht feststellen kann, indem er die in §§ 28 Abs. 1 S. 1 Nr. 2, 29 Abs. 1 Nr. 1 BDSG geforderte Interessenabwägung nicht vornehmen kann. In diesem Fall soll doch eine gestufte kollektive Verantwortlichkeit vorliegen, *Dies./Ders.*, a.a.O., S. 361; dem zustimmend auch: *Kroschwald*, ZD 2013, 388 (389).

584 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 355.

585 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 355.

586 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 361.

verantwortlich, während der Plattformbetreiber diese Daten „grundsätzlich ohne eine detaillierte Interessenabwägung“ verwenden dürfe.[587]

Diese Argumentation überzeugt nicht. Sollte die im Folgenden vorzunehmende Analyse ergeben, dass die Anbieter – wie auch von *Jandt* und *Roßnagel* angenommen[588] – die von den Nutzern übermittelten Inhaltsdaten über Dritte erheben und speichern, so können diese sich ihrer datenschutzrechtlichen Verantwortlichkeit nicht mit dem Argument entziehen, dass eine solche zu Pflichten führen würde, die in ihrem Geschäftsmodell nicht einzuhalten seien. Vielmehr würde es sich schlicht um ein insoweit rechtswidriges Geschäftsmodell handeln.[589]

Ihrem technologieneutralen Ansatz folgend, definiert die DS-GVO nicht näher, was konkret unter den einzelnen Verarbeitungsschritten zu verstehen ist. Stattdessen wird in Art. 4 Nr. 2 DS-GVO nur schlagwortartig aufgezählt, was beispielsweise eine Datenverarbeitung darstellen könnte, unter anderem die Speicherung und Erhebung von Daten. Auch an dieser Stelle bietet sich daher für eine strukturiertere Untersuchung ein Rückgriff auf die detaillierteren Normen des BDSG an, welche die mit Art. 4 Nr. 2 DS-GVO weitgehend inhaltsgleiche Regelung des Art. 2 lit. b) DSRL umsetzen.

Grundsätzlich liegt ein Erheben von Daten i.S.d. § 3 Abs. 3 BDSG nur vor, wenn aktiv Daten über einen Betroffenen beschafft werden und die Erlangung der Kenntnis von einem entsprechenden Willen getragen ist.[590] Das bloße Bereithalten eines Webformulars, in dem inhaltlich nicht vorstrukturiert Inhalte eingegeben werden können, soll nach allgemeiner Auffassung nicht ausreichen, um den Tatbestand des Erhebens zu erfüllen.[591] Auch § 14 Abs.

---

587 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 361. Es bleibt unklar, ob dies neben der Speicherung und Bereithaltung dieser nutzergenerierten Daten über Dritte sogar für eine weitere Verarbeitung durch den Anbieter etwa zu Werbezwecken gelten soll. Zwar gehen *Jandt/Roßnagel* zumindest implizit davon aus, dass der Anbieter mangels eines Einflusses der Nutzer hierfür verantwortlich wäre, a.a.O. S. 358 f. Allerdings wird auch darauf verwiesen, dass Daten, die in sozialen Netzwerken veröffentlicht wurden, ggf. allgemein zugänglich im Sinne von § 29 Abs. 1 Nr. 1 BDSG sein können, wenn die Sichtbarkeit vom Profilinhaber nicht auf seine „Freunde“ beschränkt wurde, a.a.O. S. 348, 351, 362 f. Hieraus könnte sich in entsprechenden Fällen eine Art Blankoscheck für Anbieter sozialer Netzwerke ergeben, Daten Dritter ohne eine nähere Prüfung weiter zu verarbeiten, mit erheblichen Eingriffen in die informationelle Selbstbestimmung der Betroffenen als Konsequenz. Selbst wenn dies nicht so verstanden werden soll, bleibt unklar, wie die notwendige Interessenabwägung in diesem Falle vorzunehmen wäre und warum die unterschiedliche Behandlung im Vergleich zur bloßen Veröffentlichung und Speicherung gerechtfertigt ist.

588 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 355.

589 Zur Nicht-Übertragbarkeit der Privilegierungen der §§ 8-10 TMG, ebenso wie der Rechtsprechung des BGH zur zivilrechtlichen Störerhaftung, noch ausführlich unten unter D.I.3.a)bb). Zu den einschlägigen Erlaubnistatbeständen in dieser Konstellation unten unter D.I.3.a)cc); ebenfalls in diese Richtung *Cebulla*, ZD 2015, 507 (508 f.).

590 *Dammann*, in: Simitis, BDSG, § 3 Rn. 102; *Buchner*, in: Taeger/Gabel, § 3 BDSG, Rn. 26.

591 *Dammann*, in: Simitis, BDSG, § 3 Rn. 104, 110; *Buchner*, in: Taeger/Gabel, § 3 BDSG, Rn. 26.

1 S. 2 BDSG zeigt, dass nicht jeder Speicherung von Daten eine Erhebung vorausgehen muss. Strukturiert eine Plattform die Art der einzustellenden Inhalte bereits maßgeblich durch ihre Gestaltung oder inhaltliche Ausrichtung vor, kann dagegen auch ohne eine direkte Kontrolle über das Einstellen der Inhalte durch die Nutzer ein Erheben des Plattformbetreibers vorliegen. Im Falle des Spickmich Urteils, in dem es um die Rechtmäßigkeit der Bewertung von Lehrern in einem Onlineportal ging, hat es der BGH beispielsweise für auf der Hand liegend erachtet, dass hier der Tatbestand des Erhebens und Speicherns vorlag.[592] Diese Problematik ist in Kontext zu setzen mit der grundsätzlichen Frage danach, wie viel Einfluss der Anbieter auf die Auswahl und den Zweck der übermittelten Daten und Informationen haben muss. Nach hier vertretener Ansicht – die sogleich näher zu begründen sein wird – ist der Auffassung zuzustimmen, dass die Übermittlung von Inhaltsdaten durch Nutzer sich für den Anbieter zugleich als eine Erhebung der Daten darstellt, für die der Anbieter datenschutzrechtlich verantwortlich ist.[593]

Eine Speicherung von personenbezogenen Daten liegt vor, wenn diese auf einem Speichermedium erfasst, aufgenommen oder aufbewahrt werden und dies zu dem Zweck der weiteren Verarbeitung oder Nutzung erfolgt.[594] Auch hier könnte daran gedacht werden, dass eine Verantwortlichkeit des Anbieters nur begründet werden kann, wenn im Einzelfall nachgewiesen wird, dass für die von Nutzern übermittelten und vom Anbieter sodann gespeicherten Daten eine solche weitere Verwendungsabsicht vorliegt. Eine derart enge Ansicht verkennt indes, dass grundsätzlich alle von Nutzern übermittelten personenbezogenen Inhaltsdaten für den Zweck der Abrufbarkeit durch andere Nutzer bereitgehalten werden und der konkrete Inhalt eines solchen Datums für den Anbieter dabei von nachrangiger Bedeutung ist.[595] Tatsächlich würde das Geschäftsmodell sozialer Netzwerke nicht ohne nutzergenerierte Inhaltsdaten funktionieren, da es weit weniger Gründe für die Nutzer gäbe, sich langfristig in dem sozialen Netzwerk aufzuhalten und dadurch weitere Daten wie Bestands-, Nutzungs- und Reichweitendaten für die Profilerstellung zu generieren.

Außerdem bezweckt der Anbieter eine Auswertung der übermittelten Inhaltsdaten zu Werbezwecken. Hierbei geht es nicht primär um eine Übermittlung der Daten an Dritte.

---

592 BGH, NJW 2009, 2888 (2890), Rn. 18 – Spickmich; in diese Richtung auch *Dammann*, in: Simitis, BDSG, § 3 Rn. 104; zustimmend für Personenbewertungsportale auch: *Kamp*, Personenbewertungsportale, S. 23.

593 Eine umfassende datenschutzrechtliche Verantwortlichkeit des Anbieters bejaht auch: *Piltz*, Soziale Netzwerke, S. 89 ff.; vgl. zudem *Dix*, in: Simitis, BDSG, § 35 Rn. 8.

594 *Dammann*, in: Simitis, BDSG, § 3 Rn. 114, 120; *Buchner*, in: Taeger/Gabel, § 3 BDSG, Rn. 28.

595 Vgl. auch *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 355.

Vielmehr erstellt insbesondere Facebook intern bestimmte Persönlichkeitsprofile seiner Nutzer und zeigt ihnen basierend auf diesen Profilen Werbeanzeigen. Ein maßgeblicher Teil des Umsatzes von Facebook wird durch den Verkauf entsprechender Werbeslots erzielt.[596]

Erst aus der Masse an Daten lässt sich ein klares Bild über einzelne Nutzer erstellen und in größere statistische Zusammenhänge einordnen. Es wäre daher zu kurz gegriffen, zur Bestimmung des Einflusses auf den Zweck der Speicherung auf die individuelle Motivation des Nutzers abzustellen. Der wirtschaftliche Wert eines sozialen Netzwerks liegt gerade in seinem gesammelten ‚Pool' an Daten über seine Nutzer, die immer neu verknüpft und ausgewertet werden können. Für den Anbieter ist es somit nicht primär relevant, welches Foto oder welchen Kommentar Nutzer A über eine andere Person veröffentlicht, sondern vielmehr, dass er dies überhaupt tut und damit ein bestimmtes eigenes Kommunikationsverhalten offenbart.[597] Zudem ist auch der konkrete Inhalt in Bezug auf die andere Person nur von sekundärer Bedeutung für den Anbieter. Wichtiger ist die Tatsache, dass über diese Person überhaupt etwas von Nutzer A veröffentlicht wurde, da dies wiederum Rückschlüsse darauf zulässt, dass diese beiden Personen eine engere Verbindung teilen, sie sich wahrscheinlich sogar im realen Leben kennen und entsprechend vielleicht auch weitere gemeinsame Bekannte und Interessen teilen. Hierdurch vervollständigt sich wiederum das Nutzerprofil aus Sicht des Anbieters, was den Wert des Nutzerprofils für Werbezwecke und Ähnliches steigert.[598]

Jandt und *Roßnagel* differenzieren zwischen zwei Zielen des Anbieters eines sozialen Netzwerks. Sein „Hauptziel" sei es, „die Daten seiner Nutzer für personalisierte Werbung auszuwerten und diese Werbemöglichkeiten zu ‚verkaufen'".[599] Hieraus abgeleitet verfolge er das Ziel, Nutzern „eine Plattform zur Verfügung zu stellen, auf der sie ‚Communities' bilden können" und somit das „zweite Ziel", „die Nutzer für seine Plattform zu interessieren und sie zur intensiven Erzeugung personenbezogener Daten zu veranlassen".[600] Diese Differenzierung trifft im Grundsatz sicherlich zu. Hieraus Unterschiede hinsichtlich der Verantwortlichkeit

---

596 Ausführlich zum ökonomischen Wert personenbezogener Daten insbesondere im Kontext von Werbung *Newman*, 40 William Mitchell L. Rev., 849 (865 ff.), 2013-2014; vgl. auch *Kutscha*, GR-Schutz im Internet, S. 12 f. m.w.N.; *Martini/Fritzsche*, VerwArch (104) 2013, 449 (453 f.); *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner, S. 425.

597 Auch *Kamp*, Personenbewertungsportale, S. 23 betont, dass Betreiber eines Personenbewertungsportals als „Herren der Daten" und damit potentiell datenschutzrechtlich Verantwortliche zu betrachten sind, wenn sie „ein eigenes Interesse am Betrieb eines Bewertungsportals haben und insoweit die gestalterische und rechtliche Hoheit ausüben"; vgl. auch BGH, NJW 2009, 2888 (2889), Rn. 18 – Spickmich.

598 *Oermann*, Das „Kommunikationspanopticum", S. 56; *Piltz*, Soziale Netzwerke, S. 91; *Newman*, 40 William Mitchell L. Rev., 849 (859 f.), 2013-2014.

599 *Jandt/Roßnagel*, ZD 2011, 160 (161).

600 *Jandt/Roßnagel*, ZD 2011, 160 (161).

herzuleiten, stellt aber eine künstliche Aufspaltung eines einheitlichen Lebenssachverhalts und Wirtschaftsvorgangs dar. Es ist dem Anbieter nicht möglich, Daten seiner Nutzung zu wirtschaftlichen Zwecken auszuwerten, sofern er diese nicht zuvor erhält. Gleichzeitig hat er keinerlei Interesse daran, den Nutzern eine Plattform zur Datenübermittlung zur Verfügung zu stellen, wenn er hierdurch nicht seine wirtschaftlichen Ziele erfüllen kann. Gemäß der jedenfalls seit dem Google-Urteil des EuGH gebotenen funktionell-wirtschaftlichen Auslegung des Begriffs der verantwortlichen Stelle[601] ist daher von einer untrennbaren Verbindung dieser Ziele und den zugehörigen Datenverarbeitungsschritten auszugehen. Eine Verantwortlichkeit des Anbieters wegen eines Erhebens gemäß § 3 Abs. 3 BDSG bzw. Speicherns gemäß § 3 Abs. 4 Nr. 1 BDSG und zukünftig Art. 4 Nr. 2 DS-GVO scheitert somit nicht daran, dass er keinen hinreichenden Einfluss auf die Zwecksetzung hat bzw. diese im Moment der Speicherung noch nicht hinreichend konkretisiert ist. Der Anbieter ist vielmehr vollständig datenschutzrechtlich verantwortlich für die Übermittlung personenbezogener Inhaltsdaten Dritter durch die Nutzer, unabhängig von einer weiteren Datenverarbeitung.[602]

Dieses Ergebnis wird weiter dadurch unterstützt, dass die Anbieter durch die Gestaltung der AGB und der Plattform erheblichen Einfluss auf die Entscheidung der Nutzer nehmen, welche Informationen diese über sich und über andere posten, auch wenn sie die konkrete Auswahl der Inhalte den Nutzern überlassen.[603] Viele Netzwerke bieten für das Ausfüllen des Nutzerprofils Formulare an, in welchem systematisch Interessen, Musikgeschmack, Aufenthaltsort, Ausbildung und weitere persönliche Daten der Nutzer abgefragt werden. Es wird die Möglichkeit geboten, Fotoalben zu veröffentlichen und „Gruppen“ beizutreten, um Interessen nach außen zu bekunden und sich als Nutzer eine Online-Selbstdarstellung bzw. ein digitales Selbstbild zu schaffen.[604] Durch die implizite Aufforderung, dieses digitale Selbst mit Leben zu erfüllen, werden Nutzer im Folgenden dazu angeregt, weitere Informationen über sich selbst, eigene Aktivitäten und insbesondere auch die ihrer Bekannten zu veröffentlichen. Gerade

601 Hierzu ausführlich oben unter C.II.4.b)bb).

602 In diese Richtung auch schon *Piltz*, Soziale Netzwerke, S. 91; vgl. auch *Dix*, in: Simitis, BDSG, § 35 Rn. 8. Zur Frage, inwieweit die Nutzer, die personenbezogene Daten Dritter in sozialen Netzwerken übermitteln, als kumulativ verantwortlich anzusehen sind, s. sogleich unter D.I.3.b); vgl. auch *Piltz/Trinkl*, in: Hoeren/Bensinger, Kap. 13, Rn. 133; *Kamp*, Personenbewertungsportale, S. 43 ff.; teilweise a.A. *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 348, 355, 361; *Kroschwald*, ZD 2013, 388 (389).

603 *Oermann*, Das „Kommunikationspanopticum“, S. 56; *Piltz/Trinkl*, in: Hoeren/Bensinger, Kap. 13, Rn. 133; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 348; *Kamp*, Personenbewertungsportale, S. 46 f.; vgl. auch *Spiecker gen. Döhmann*, K&R 2012, 717 (718); *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 63.

604 *Grimmelmann*, 94 Iowa L.Rev. 1137 (1149 ff.), 2008-2009; *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 32 f., 34.

Verknüpfungen mit anderen Nutzern oder Dritten, die nicht Mitglied in dem sozialen Netzwerk sind, haben für die Anbieter noch einmal gesteigerten Wert, da sich aus den Beziehungen zu diesen Freunden wiederum Rückschlüsse auf eigene Interessen des Nutzers ziehen lassen, vielleicht sogar ohne dass sich dieser dessen bewusst ist.[605]

Im Ergebnis besteht somit eine wirtschaftlich-funktionelle Einheit zwischen den nutzergenerierten Inhaltsdaten – auch über Dritte – und dem auf Speicherung, Abrufbarkeit und späterer Auswertung und teilweisem Verkauf dieser Daten beruhenden Geschäftsmodell der Anbieter sozialer Netzwerke. Die Anbieter bestimmen zwar nicht im Einzelnen, welche nutzergenerierten Inhalte erzeugt werden, setzen aber bestimmte Anreize und strukturieren die Art der Inhalte durch die Plattformgestaltung. Sie kontrollieren daher den primären wirtschaftlichen Zweck der Datenerhebung und delegieren lediglich die Mittel der Erhebung an die Nutzer.[606] Jedenfalls in der gebotenen weiten wirtschaftlich-funktionellen Begriffsauslegung sind sie daher als datenschutzrechtlich verantwortliche Stelle für die Erhebung und Speicherung nutzergenerierter Inhaltsdaten einzustufen. Sie sind in dieser Hinsicht vollumfänglich Adressaten der datenschutzrechtlichen Regelungen und Pflichten.[607]

bb) Keine Übertragung der Regelungen in §§ 7 ff. TMG sowie der Grundsätze der zivilrechtlichen Störerhaftung

Es wird unter Verweis auf die haftungsrechtlichen Privilegierungen der §§ 8-10 TMG vertreten, die datenschutzrechtliche Verantwortlichkeit der Anbieter sozialer Netzwerke einzuschränken, wenn diese faktisch keine Möglichkeit haben, die in §§ 28 Abs. 1 S. 1 Nr. 2, 29 Abs. 1 Nr. 1 BDSG geforderte Interessenabwägung vorzunehmen.[608] Das Recht dürfe keine unmöglichen Pflichten auferlegen. Der Datenschutz sei vielmehr dadurch zu gewährleisten, dass insoweit

605 Hierzu schon ausführlich oben unter B.II.

606 So auch *Piltz*, Soziale Netzwerke, S. 91; vgl. auch bereits *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner, S. 427.

607 Vgl. auch *Piltz*, Soziale Netzwerke, S. 89 ff.; *Piltz/Trinkl*, in: Hoeren/Bensinger, Kap. 13, Rn. 131 ff.; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 82 ff.; *Dix*, in: Simitis, BDSG, § 35 Rn. 8; *Buchner*, in: Taeger/Gabel, § 3 BDSG Rn. 52; für strukturell vergleichbare Betreiber von Personenbewertungsportalen: *Kamp*, Personenbewertungsportale, S. 47; teilweise a.A. *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 348 ff., welche zwar die Verantwortlichkeit des Anbieters für die Erhebung und Speicherung bejahen, diese aber weitgehend einschränken wollen, soweit eine Kontrolle der nutzergenerierten Inhalte im Einzelfall nicht möglich ist.

608 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 361; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 83 weist ebenfalls auf die Schwierigkeiten dieser Interessenabwägung hin, verweist aber zurecht darauf, dass diese letztlich unbeachtlich sind, da eine Anbieterverantwortlichkeit erst besteht, sofern ein Anbieter seine „neutrale Stellung" als bloßer Vermittler von Inhalten verlässt, indem – wie auch oben bereits beschrieben – ein relevanter Einfluss auf die Mittel und Zwecke der Datenverarbeitung durch eigene Datenverarbeitungsprozesse genommen wird.

den die Inhaltsdaten einstellenden Nutzern eine volle Verantwortlichkeit für diese Daten zukomme.[609]

Dem ist indes nicht zu folgen. Unabhängig von der Verantwortlichkeit der Nutzer für die Übermittlung der Inhaltsdaten ist die Übertragung der Privilegierungen der §§ 8-10 TMG abzulehnen.[610] Eine Übertragung übergeht die unterschiedliche Schutzrichtung der datenschutzrechtlichen Regelungen und jener Privilegierungen und verkennt, dass es sich bei den datenschutzrechtlichen Regelungen zu Recht um *lex specialis* handelt. Nach einem kurzen Überblick über die Regelungen der §§ 7 ff. TMG soll dies im Folgenden gezeigt werden.

i) Unanwendbarkeit der §§ 7 ff. TMG auf Unterlassungsansprüche

Die Regelungen der §§ 7 ff. TMG stellen keine eigenständigen Anspruchsgrundlagen dar, sondern setzen eine Verantwortlichkeit nach allgemeinen Vorschriften voraus.[611] Ihre dogmatische Einordnung ist umstritten.[612] Nach einer weit verbreiteten Meinung sind sie gleichsam als Filter einer möglichen Haftung vorweg zu prüfen.[613] Dem wird indes zu Recht vorgeworfen, dass es sich um eine systemfremde Ebene der Vorprüfung handelt[614], so dass es stringenter erscheint, sie im Rahmen des Zurechnungszusammenhangs in die jeweiligen Haftungstatbestände zu integrieren.[615] Für die hier betrachteten Fragen ergibt sich indes im Ergebnis kein Unterschied, da die §§ 7 ff. TMG nach beiden Ansichten herangezogen werden können, um privilegierend den Zurechnungszusammenhang für eine ansonsten rechtswidrige Handlung zu unterbrechen. Daher soll hier nicht vertiefend auf diesen Streit eingegangen werden. Als horizontale Regelungen gelten sie – jedenfalls nach herrschender Auffassung – für alle Teilrechtsordnungen, also grundsätzlich sowohl für strafrechtliche, als auch ordnungsrechtliche und zivilrechtliche Haftungsfragen.[616]

---

609 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 361.

610 So auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 83.

611 *Altenhain*, in: MüKo-StGB, Bd. 7, Vor §§ 7 ff. TMG, Rn. 2; *Hoffmann*, in: Spindler/Schuster, Vor §§ 7 ff. TMG, Rn. 25; *Schapiro*, Unterlassungsansprüche, S. 321 m.w.N.

612 Einen ausführlichen Meinungsüberblick bieten *Schapiro*, Unterlassungsansprüche, S. 322 ff. und *Altenhain*, in: MüKo-StGB, Bd. 7, Vor §§ 7 ff. TMG, Rn. 5 ff.

613 Statt vieler *Altenhain*, in: MüKo-StGB, Bd. 7, Vor §§ 7 ff. TMG, Rn. 5, 7 m. zahlreichen w.N.; *Moos*, in: Taeger/Gabel, Einf TMG, Rn. 17.

614 *Hoffmann*, in: Spindler/Schuster, Vor §§ 7 ff. TMG, Rn. 30 ff.; *Schapiro*, Unterlassungsansprüche, S. 329 f.

615 *Hoffmann*, in: Spindler/Schuster, Vor §§ 7 ff. TMG, Rn. 32; *Schapiro*, Unterlassungsansprüche, S. 330 f.

616 *Altenhain*, in: MüKo-StGB, Bd. 7, Vor §§ 7 ff. TMG, Rn. 2 m.w.N.; *Hoffmann*, in: Spindler/Schuster, Vor §§ 7 ff. TMG, Rn. 25; *Schapiro*, Unterlassungsansprüche, S. 312 m.w.N.; vgl. auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 83.

Allerdings ist das rechtliche Verhältnis der §§ 7 ff. TMG zur zivilrechtlichen Störerhaftung nicht abschließend geklärt.[617] Nach bisher ständiger Rechtsprechung des BGH finden die Privilegierungen der §§ 8-10 TMG keine Anwendung auf Unterlassungsansprüche, die im Rahmen der zivilrechtlichen Störerhaftung u.a. gemäß § 1004 Abs. 1 BGB geltend gemacht werden.[618] Ob dies wirklich unionsrechtskonform ist, wird teilweise in Frage gestellt, da der EuGH die zugrundeliegenden Richtlinienbestimmungen, insbesondere Art. 14 ECRL, in Fällen von Unterlassungsklagen angewandt hat, allerdings ohne sich mit dem Problem auseinanderzusetzen.[619] Eine Unionsrechtswidrigkeit der Rechtsprechung des BGH folgt hieraus allerdings keinesfalls zwingend, da hinsichtlich der mittelbaren Verantwortlichkeit von Intermediären vieles unionsrechtlich offen gelassen wird und auch Art. 14 ECRL insoweit keine strengen Vorgaben macht, wie die vorgegebene Haftungsbeschränkung in nationales Recht umzusetzen ist. Den Mitgliedstaaten bleibt somit ein erheblicher Spielraum bei der Gestaltung ihrer Rechtsordnungen; der deutsche Weg der zivilrechtlichen Störerhaftung ist hierbei nur ein Regelungsmodell unter vielen.[620] Im Rahmen der Beschränkung dieser Störerhaftung greift die Rechtsprechung – wenngleich ohne ausdrücklich hierauf einzugehen – auf die Kriterien des Art. 14 ECRL zurück, hierzu sogleich. Aufgrund des nationalen Umsetzungsspielraums wird an dieser Stelle daher davon ausgegangen, dass eine Nichtanwendung der §§ 8-10 TMG auf Unterlassungsansprüche keinen Verstoß gegen Unionsrecht darstellt, solange eine Beschränkung der zivilrechtlichen Störerhaftung durch die dogmatische Konstruktion derselben sichergestellt ist.[621]

---

617 Instruktiv *Ohly*, ZUM 2015, 308 (312 f.) m.w.N.; *Chmelik*, Social Network Sites, S. 271 ff. Eine abschließende Klärung ist auch nicht durch das Dritte Gesetz zur Änderung des Telemediengesetzes vom 13. Oktober 2017 erfolgt, welches die Störerhaftung für Access-Provider nach § 8 Abs. 1 S. 2 TMG, insbesondere WLAN-Betreiber, abschaffte und als Ersatz einen Anspruch auf Netzsperren bei Urheberrechtsverletzung u.Ä. gemäß § 7 Abs. 4 TMG normierte. Instruktiv hierzu *Spindler*, NJW 2017, 2305 (2308).

618 Mittlerweile ständige Rechtsprechung des BGH, vgl. BGH, NJW 2009, 2888 (2889), Rn. 14 – Spickmich; BGH, NJW 2007, 2558 (2559), Rn. 7 m.w.N.; BGHZ 158, 236 (246 ff.) – Internetversteigerung I; *Hoffmann*, in: Spindler/Schuster, § 10 TMG, Rn. 3; *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1., Rn. 89; *Hollenders*, Mittelbare Verantwortlichkeit, S. 227; *Moos*, in: Taeger/Gabel, Einf TMG, Rn. 19 f.; ausführlich: *Schapiro*, Unterlassungsansprüche, S. 363 ff., 381 ff.; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 64 f.; *Chmelik*, Social Network Sites, S. 272 ff.; kritisch und teilweise a.A.: *Ohly*, ZUM 2015, 308 (312); *Hoeren*, in: FS Eisenhardt, S. 250 ff. *Chmelik*, Social Network Sites, S. 272 ff.

619 EuGH, *Google France*, Rs. C-236/08 bis C-238/08, Rn. 112 ff.; *Ohly*, ZUM 2015, 308 (312); in diese Richtung auch *Hollenders*, Mittelbare Verantwortlichkeit, S. S. 229 ff., 240 ff., mit dem zentralen Argument, dass eine höhere Rechtssicherheit zu erwarten ist, wenn Unterlassungsansprüche den gesetzlich normierten §§ 7 ff. TMG unterfallen anstatt richterrechtlichen allgemeinen Haftungsgrundsätzen. Ausführlich hierzu auch *Chmelik*, Social Network Sites, S. 168 ff., welcher die Störerhaftung sogar als „geboten[e]“ Ergänzung der unionsrechtlichen Regelungen bezeichnet.

620 *Ohly*, ZUM 2015, 308 (310 ff.) m.w.N.; vgl. auch *Peifer*, AfP 2014, 18 (19 f.); vgl. auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 64 f.

621 So auch *Peifer*, AfP 2014, 18 (20); kritisch: *Ohly*, ZUM 2015, 308 (312).

Grundsätzlich kann als Störer bei der Verletzung absoluter Rechte in Anspruch genommen werden, „wer – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechts beiträgt“.[622] Diese Störerhaftung hat im telemedienrechtlichen Bereich insbesondere Bedeutung für die Betreiber von Internetauktionshäusern wie eBay, aber auch sonstigen Content-Providern, die beispielsweise Musik, Fotos oder Filme zum Download anbieten. Dabei handelt es sich in der Regel um eine mittelbare Störereigenschaft, die dadurch gekennzeichnet ist, dass die Diensteanbieter ihren Nutzern die Möglichkeit bieten, potentiell rechtswidrige Inhalte hochzuladen und zu verbreiten.[623] Hier liegt die Parallele zu den Anbietern sozialer Netzwerke.[624]

Da die Störerhaftung kein Verschulden voraussetzt, besteht ein starkes Bedürfnis, die Verantwortlichkeit und den Zurechnungszusammenhang anderweitig einzuschränken. Die Ansicht des BGH, dass diese Einschränkung nicht über die Privilegierungen der §§ 8-10 TMG erfolgen kann, überzeugt. Man könnte annehmen, dass bereits der Wortlaut des § 7 Abs. 3 S. 1 TMG einer solchen Privilegierung entgegensteht, da er auch bei einer Nichtverantwortlichkeit nach den §§ 8-10 TMG eine Verpflichtung zur Entfernung oder Sperrung der Nutzung von Informationen statuiert. Der Wortlaut ist indes nicht eindeutig: In enger Auslegung lässt sich vertreten, dass sich diese Begrenzung der Privilegierungen der §§ 8-10 TMG nur auf bereits eingetretene Rechtsverletzungen bezieht.[625] Andererseits ist durch die Verpflichtung zur Sperrung der Nutzung der Informationen eine Wirkung in die Zukunft angelegt, so dass eine Ausweitung auf zukunftsgerichtete Unterlassungsansprüche jedenfalls möglich erscheint.[626]

Eine Anwendung der §§ 8-10 TMG auf Unterlassungsansprüche ist aber auch aus systematischen Erwägungen abzulehnen, da sie zu nicht hinnehmbaren Wertungswidersprüchen führen würde: § 10 Abs. 1 Nr. 1 2. Hs. TMG senkt explizit die Anforderungen an einen Schadensersatzanspruch gegenüber sonstigen Verantwortlichkeiten des Diensteanbieters für fremde Informationen, so dass ein Schadensersatzanspruch im Ergebnis leichter durchzusetzen wäre als ein Unterlassungsanspruch, fiele dieser unter § 10 Abs. 1 Nr. 1 1. Hs. TMG.[627] Eine in ihren Rechten verletzte Person könnte daher gegebenenfalls

---

622 BGH, GRUR 2011, 152 (155), Rn. 45 – Kinderhochstühle im Internet I, m.w.N; siehe auch *Fritzsche*, in: Bamberger/Roth, BGB, Bd. 2, § 1004 BGB Rn. 15, m.w.N.

623 Vgl. *Fritzsche*, in: Bamberger/Roth, BGB, Bd. 2, § 1004 BGB Rn. 17 f.

624 Vgl. auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 65; sehr ausführlich zur Haftung von Anbietern sozialer Netzwerke für nutzergenerierte Inhalte auf Grundlage der ECRL und den §§ 7 ff. TMG *Chmelik*, Social Network Sites, S. 85 ff., S. 141 ff.

625 Vgl. *Schapiro*, Unterlassungsansprüche, S. 382.

626 *Schapiro*, Unterlassungsansprüche, S. 382 f.

627 BGHZ 158, 236 (246 ff.) – Internetversteigerung I; ausführlich: *Schapiro*, Unterlassungsansprüche, S. 385.

einen Schadensersatzanspruch für eine erfolgte Rechtsverletzung erhalten, ihr Eintreten aber nicht mittels eines Unterlassungsanspruchs verhindern. Das Recht sollte aber niemanden verpflichten, eine rechtswidrige Verletzungshandlung zunächst zu dulden, für die im Nachhinein ein Schadensersatzanspruch gewährt wird.[628] Die §§ 8-10 TMG können daher nicht zur Begrenzung der zivilrechtlichen Störerhaftung von Diensteanbietern herangezogen werden.[629]

ii) Begrenzung der zivilrechtlichen Störerhaftung

Um die mittelbare Störerhaftung „nicht über Gebühr" auf Diensteanbieter wie Content-Provider und Betreiber von Internetauktionsplattformen – und damit potentiell auch Anbieter sozialer Netzwerke – zu erstrecken, setzt die Rechtsprechung stattdessen eine „Verletzung zumutbarer Verhaltenspflichten, insbesondere von Prüfpflichten" voraus.[630] Die Zumutbarkeit ist hierbei jeweils im Einzelfall zu beurteilen, wobei es von Bedeutung sein kann, ob der als Störer in Anspruch Genommene eigene Gewinnerzielungsabsichten verfolgt und ob eine geförderte Rechtsverletzung eines Dritten offenkundig oder nur schwer zu erkennen war.[631] Eine allgemeine, anlasslose Prüfpflicht für sämtliche von Kunden und Nutzern eingestellten Inhalte ist dabei gemäß § 7 Abs. 2 TMG ausgeschlossen[632] und darüber hinaus auch nach dem zugrundeliegenden Art. 15 Abs. 1 ECRL europarechtlich unzulässig.[633] Eine Prüfpflicht und entsprechend auch eine zivilrechtliche Haftung als Störer kommen daher im Wesentlichen erst in Betracht, wenn der Verantwortliche entweder auf eine konkrete Rechtsverletzung

628 *Schapiro*, Unterlassungsansprüche, S. 386.

629 Ständige Rechtsprechung des BGH, vgl. BGH, NJW 2009, 2888 (2889), Rn. 14 – Spickmich; BGH, NJW 2007, 2558 (2559), Rn. 7 m.w.N.; BGHZ 158, 236 (246 ff.) – Internetversteigerung I; *Hoffmann*, in: Spindler/Schuster, § 10 TMG, Rn. 3; *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1., Rn. 89; ausführlich: *Schapiro*, Unterlassungsansprüche, S. 363 ff., 381 ff.; *Chmelik*, Social Network Sites, S. 271 ff.; kritisch und teilweise a.A. *Ohly*, ZUM 2015, 308 (312); *Hoeren*, in: FS Eisenhardt, S. 250 ff.

630 Ständige Rechtsprechung des BGH, statt vieler BGH, GRUR 2013, 1229 (1231), Rn. 34 – Kinderhochstühle im Internet II, m.w.N.; *Hoffmann*, in: Spindler/Schuster, § 10 TMG, Rn. 4; *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1., Rn. 89; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 65 ff.

631 BGH, GRUR 2013, 1229 (1231), Rn. 34 – Kinderhochstühle im Internet II, m.w.N.

632 BGH, GRUR 2013, 1229 (1231), Rn. 36 – Kinderhochstühle im Internet II, m.w.N.; BGH, GRUR 2015, 485 (490), Rn. 51 – Kinderhochstühle im Internet III; *Altenhain*, in: MüKo-StGB, Bd. 7, Vor §§ 7 ff. TMG, Rn. 5 f.; *Moos*, in: Taeger/Gabel, Einf TMG, Rn. 18; *Hollenders*, Mittelbare Verantwortlichkeit, S. 230 ff.; *Schapiro*, Unterlassungsansprüche, S. 395, 407 ff.

633 EuGH, *L'Oréal/Ebay*, Rs. C-324/09, Rn. 139 = GRUR 2011, 1025 (1034); *Hollenders*, Mittelbare Verantwortlichkeit, S. 230 f.; *Schapiro*, Unterlassungsansprüche, S. 394 ff.; *Peifer*, AfP 2014, 18 (20); vgl. auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 66.

hingewiesen wurde[634] oder er seine „neutrale Stellung" als Vermittler von Inhalten aufgegeben hat[635]. Dies entspricht den Vorgaben der Art. 14, 15 ECRL. Wann diese Voraussetzungen im Einzelfall vorliegen, ist indes häufig unklar, so dass hier eine erhebliche Rechtsunsicherheit besteht.[636]

iii) Von einer Verletzung konkreter Prüfpflichten unabhängige datenschutzrechtliche Verantwortlichkeit

Weder die Privilegierungen der §§ 8-10 TMG noch die soeben skizzierten einschränkenden Prüfpflichten bei der zivilrechtlichen Störerhaftung sind auf die datenschutzrechtliche Verantwortlichkeit der Anbieter sozialer Netzwerke für nutzergenerierte Inhaltsdaten zu übertragen. Die datenschutzrechtlichen Regelungen stellen vielmehr spezielle Regelungen dar, die jenen Regelungen vorgehen.[637] Durch technische Neuerungen hat sich keine neue Situation ergeben, die eine Lücke begründen und damit ein Abweichen von den restriktiven Datenschutzgesetzen zugunsten einer Analogie zu der Störerhaftung erforderlich machen würde. Als maßgebliche Konsequenz besteht die datenschutzrechtliche Verantwortlichkeit von Anbietern sozialer Netzwerke für nutzergenerierte Inhaltsdaten über Dritte gegebenenfalls auch ohne die Verletzung von zumutbaren Prüfpflichten.

(1) Keine unmittelbare Anwendbarkeit der §§ 7 ff. TMG auf die datenschutzrechtliche Verantwortlichkeit

Die Systematik des TMG, welches die die datenschutzrechtlichen Verpflichtungen in einem gesonderten Kapitel in den §§ 11 ff. TMG regelt[638], stellt bereits ein Indiz für das Spezialverhältnis von datenschutzrechtlicher Verantwortlichkeit gegenüber der Haftung nach

634 BGH, BGHZ 191, 19 (26), Rn. 21 – Stiftparfüm; vgl. auch BGH, NJW 2012, 148 (150); BGH, MMR 2009, S. 752 (753); BGH, NJW-RR 2008, 1136 (1138 ff.) – Internetversteigerung III; BGH, BGHZ 172, 119 (130 ff.) – Internetversteigerung II; BGH, BGHZ 158, 236 (246 ff.) – Internet-Versteigerung I; BGH, BGHZ 148, 13, 17 f. – ambiente.de; instruktiv: *Sieber/Höfinger*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 18.1., Rn. 82 ff.; *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1., Rn. 89; *Schapiro*, Unterlassungsansprüche, S. 390 ff.; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 66 f.

635 BGH, GRUR 2013, 1229 (1231), Rn. 37, 48 ff. – Kinderhochstühle im Internet II m.w.N.; BGH, NJW 2009, 2888 (2889), Rn. 14 – Spickmich; *Spindler*, Störerhaftung im Internet, in: FS Köhler (Alexander u.a., Hrsg.), S. 710; *ders.*, Gutachten F zum 69. dt. Juristentag, 2012, S. 62 ff.; *Peifer*, AfP 2014, 18 (19 f.).

636 Ausführlich *Spindler*, Störerhaftung im Internet, in: FS Köhler (Alexander u.a., Hrsg.), S. 697 ff.; *Schapiro*, Unterlassungsansprüche, S. 232 ff., 265 ff.

637 So auch *Moos*, in: Taeger/Gabel, Einf TMG, Rn. 21; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 83. Entsprechend ist es an dieser Stelle nicht entscheidend, inwiefern die Anbieter sozialer Netzwerke zivilrechtlich als Störer einzustufen wären. Vgl. hierzu allerdings instruktiv *Chmelik*, Social Network Sites, S. 157 ff., welcher im Ergebnis eine Störereigenschaft der Anbieter für rechtsverletztende Inhalte der Nutzer und damit eine mögliche Haftung nach den Vorgaben der zivilrechtlichen Störerhaftung bejaht.

638 Vgl. zum Verhältnis der §§ 11 ff. TMG und der DS-GVO bereits oben unter C.I.2.

den allgemeinen Vorschriften gemäß § 7 TMG bzw. den Privilegierungen der §§ 8-10 TMG dar. § 12 Abs. 3 TMG bestimmt abweichend von § 7 TMG, dass für den Umgang mit personenbezogenen Daten die hierfür geltenden Vorschriften anzuwenden sind. In Ermangelung einer gesonderten Definition für die datenschutzrechtliche Verantwortlichkeit muss daher auf § 3 Abs. 7 BDSG zurückgegriffen werden.[639] Dies entspricht dem zugrundeliegenden Art. 1 Abs. 5b ECRL i.V.m. Erwägungsgrund Nr. 14 ECRL, wonach die Datenschutzrichtlinien 95/46/EG und 97/66/EG[640] vom Anwendungsbereich der ECRL ausgenommen sein sollten. Auch historisch war eine Regelung der datenschutzrechtlichen Verantwortlichkeit durch die §§ 7 ff. TMG mithin nicht beabsichtigt.[641] Dieser gesetzgeberische Gedanke wird in Zukunft auch auf die DS-GVO als Nachfolgeregelung der DSRL zu übertragen sein, so dass es keine Anhaltspunkte dafür gibt, zu untersuchen, inwieweit die §§ 7 ff. TMG als nationales Recht, das der Umsetzung der ECRL diente, zur Einschränkung der DS-GVO herangezogen werden könnten.

Neben diesem historischen Argument finden sich im TMG zudem keine speziellen Regelungen für Inhaltsdaten, so dass auch insoweit subsidiär auf die Regelungen des BDSG – und zukünftig der DS-GVO – zurückzugreifen ist[642] und sich keine Konkurrenzprobleme zwischen dem TMG und dem BDSG ergeben. Eine Beschränkung der datenschutzrechtlichen Verantwortlichkeit durch die §§ 7 ff. TMG wäre entsprechend bereits bisher und auch zukünftig systemwidrig.[643]

Auch teleologisch überzeugt es nicht, die datenschutzrechtliche Verantwortlichkeit von der Verletzung zumutbarer Prüfpflichten abhängig zu machen. Die Vorschriften des BDSG und der DS-GVO sichern insbesondere die informationelle Selbstbestimmung der von der Datenverarbeitung betroffenen Person, indem dieser Auskunfts-, Berichtigungs- und Löschungsansprüche zugestanden werden. Sie verbieten zudem, dass personenbezogene Daten ohne gesetzliche Grundlage bzw. ohne Einwilligung der betroffenen Person verarbeitet und weitergegeben werden. Diese im allgemeinen Persönlichkeitsrecht wurzelnden Rechte sind in ihrem Bestand unabhängig von der inhaltlichen Richtigkeit der Daten und sichern das Recht

639 *Moos*, in: Taeger/Gabel, § 11 Rn. 28; AK I „Staatsrecht und Verwaltung“, Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 16; vgl. auch *Spindler/Nink*, in: Spindler/Schuster, § 12 TMG, Rn. 8; *Kamp*, Personenbewertungsportale, S. 37 ff., 50.

640 Richtlinie 97/66/EG des europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation.

641 Vgl. *Hoffmann*, in: Spindler/Schuster, Vor §§ 7 ff. TMG, Rn. 14; *Moos*, in: Taeger/Gabel, Einf. TMG, Rn. 21; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 83.

642 Hierzu ausführlich oben unter C.III.4.

643 Im Ergebnis so auch schon *Kamp*, Personenbewertungsportale, S. 36, 48 ff.; vgl. auch *Hoffmann*, in: Spindler/Schuster, Vor §§ 7 ff. TMG, Rn. 14; *Moos*, in: Taeger/Gabel, Einf. TMG, Rn. 20 f.

des Einzelnen zur kontrollierten Selbstdarstellung.[644] Es besteht insoweit ein relevanter, struktureller Unterschied zu den Regelungen insbesondere des Zivilrechts: Während in zivilrechtlichen Verhältnissen Geschäftspraktiken grundsätzlich erlaubt sind, solange sie nicht rechtswidrig einen anderen in seinen absoluten Rechten verletzen, also etwa in seinem Urheberrecht, existiert im Datenschutzrecht ein Verbot mit Erlaubnisvorbehalt gemäß § 4 Abs. 1 BDSG bzw. Art. 7 DSRL und zukünftig Art. 6 Abs. 1 DS-GVO. Im Zivilrecht würde eine allgemeine Prüfpflicht für nutzergenerierte Inhalte bedeuten, im Zweifel eigene bestehende Verhaltensfreiheiten einzuschränken, um sich nicht einem Haftungsrisiko auszusetzen. Dies ist unverhältnismäßig und wird daher mit Recht abgelehnt.[645] Zudem handelt es sich gerade bei der Bereitstellung von entsprechenden Internet-Plattformen um grundsätzlich sozial erwünschte Tätigkeiten, so dass auch insoweit eine Haftungseinschränkung angezeigt ist.[646] Im öffentlich-rechtlichen Datenschutzrecht kann angesichts des geltenden Verbots mit Erlaubnisvorbehalt gerade nicht davon ausgegangen werden, dass eine grundsätzliche Berechtigung zur Erhebung und Speicherung von personenbezogenen Daten besteht. Der Datenverarbeiter ist vielmehr dazu angehalten, sich vor der Verarbeitung eben dieser Berechtigung zu versichern.

Diese restriktive Regelung folgt aus der abstrakten Gefährlichkeit des Umgangs mit personenbezogenen Daten für die informationelle Selbstbestimmung Betroffener.[647] Anders als bei der zivilrechtlichen Haftungsfrage geht es nicht darum, was konkret veröffentlicht wurde und ob hierdurch absolute Rechte des Betroffenen rechtswidrig und schuldhaft verletzt wurden. Entscheidend ist vielmehr, dass überhaupt personenbezogene Daten über Dritte veröffentlicht wurden und hieraus eine Gefährdung ihrer informationellen Selbstbestimmung resultiert. Der Anbieter des sozialen Netzwerks ist durch die Speicherung der Daten und durch die Zurverfügungstellung für weitere Nutzer verantwortlich für die Weiterverbreitung dieser Daten und damit eine Verstärkung der Verletzung der informationellen Selbstbestimmung. Dies stellt exakt die Gefährdung der informationellen Selbstbestimmung dar, für welche die Regelungen des BDSG erlassen wurden. Es kann daher nicht privilegierend wirken, wenn der Anbieter die von Nutzern übermittelten personenbezogenen Daten Dritter im Einzelfall nicht auf ihre

644 Vgl. *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 166, 178; *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 568 ff.; vgl. auch *Simitis*, in: Simitis, BDSG, § 1 Rn. 24 f., welcher allerdings dogmatisch die Eigenständigkeit des Rechts auf informationelle Selbstbestimmung betont und in der Verknüpfung mit dem allgemeinen Persönlichkeitsrecht vor allem eine Quelle für Missverständnisse sieht.

645 *Peifer*, AfP 2014, 18 (20 f.) m.w.N.

646 *Ohly*, ZUM 2015, 308 (311).

647 Vgl. *Peifer*, K&R 2011, 543 (545).

Richtigkeit überprüfen kann. Die datenschutzrechtlichen Regelungen haben insoweit einen Risikovorsorge-Charakter[648]: Wer die abstrakt gefährliche Handlung des Umgangs mit personenbezogenen Daten vornimmt, muss sicherstellen, dass dies in Übereinstimmung mit den erlassenen Schutzvorschriften geschieht. Kann dies nicht sichergestellt werden, so ist der Umgang gegebenenfalls zu unterlassen. Dies ist der Wesensgehalt eines Verbots mit Erlaubnisvorbehalt.[649] Solange dies geltendes Recht ist, können sich die Anbieter sozialer Netzwerke ihrer datenschutzrechtlichen Verantwortlichkeit für die Verarbeitung nutzergenerierter personenbezogener Inhaltsdaten über Dritte nicht dadurch entziehen, dass sie diese im Einzelnen nicht kontrollieren können.

Im Ergebnis bedeutet dies, dass eine anlasslose Prüfpflicht für personenbezogene, nutzergenerierte Inhaltsdaten über Dritte besteht, sofern der Anbieter des sozialen Netzwerks hinreichende Kontrolle über die Zwecke und Mittel Datenverarbeitung ausübt, um selbst als datenschutzrechtlich Verantwortlicher zu gelten. Dem steht nicht die Regelung des § 7 Abs. 2 TMG entgegen, da diese, wie soeben festgestellt, nicht auf die datenschutzrechtliche Verantwortlichkeit anwendbar ist.

(2) Keine analoge Anwendbarkeit der §§ 7 ff. TMG oder Übertragung des Rechtsgedankens

Das Verbot der anlasslosen Prüfpflicht aus § 7 Abs. 2 TMG bzw. der dahinterstehende Rechtsgedanke sind auch nicht analog auf die datenschutzrechtliche Verantwortlichkeit anzuwenden.

Sinn und Zweck des Verbots der anlasslosen Prüfpflicht ist, dass es andernfalls zu einer verschuldensunabhängigen Haftung für fremdes Verhalten käme und die ganz überwiegende

---

[648] Hierzu noch unten unter E.II; vgl. auch *Fehling*, Privacy, in: ders. u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 137 ff. – *Erscheinen in Vorbereitung*.

[649] Das Verbot mit Erlaubnisvorbehalt im Datenschutzrecht wird zuweilen stark kritisiert, *Härting/Schneider*, ZRP 2011, 233 (234) bezeichnen es gar als eine Art „Kommunikationsverbot – mit Erlaubnisvorbehalt"; in diese Richtung auch *Masing*, NJW 2012, 2305 (2307). Diese Kritik ist indes deutlich zu hart; angesichts massiver Informations- und Machtgefälle zwischen großen datenverarbeitenden Unternehmen und privaten Nutzern ist die Annahme einer gleichberechtigten Aushandlung von Datennutzungsbefugnissen und die Forderung nach transparenter Datenverarbeitung, die von dem Betroffenen kontrolliert werden kann, unrealistisch. Das Verbot mit Erlaubnisvorbehalt stellt eine staatliche Schutzregel dar, die den Betroffenen im Ausgangspunkt zum Herrn seiner Daten erklärt und klarstellt, dass eine Erhebung oder Verarbeitung nur in gesetzlich geregelten Ausnahmefällen oder mit ausdrücklicher Einwilligung des Betroffenen geschehen darf, vgl. auch *Karg*, DuD 2013, 75 (77 ff.). Zudem entzieht das „Haushaltsprivileg" des § 1 Abs. 2 Nr. 3 BDSG bzw. Art. 2 Abs. 2 lit. c) DS-GVO Datenverarbeitungen zu rein persönlichen und familiären Zwecken dem Anwendungsbereich des Datenschutzrechts, so dass für einen Großteil der privaten Kommunikation keine datenschutzrechtlichen Einschränkungen bestehen. (Zu Besonderheit der privaten Kommunikation in sozialen Netzwerken vgl. allerdings ausführlich unten unter D.I.3.b)aa)).

Mehrheit der Dienstleistungen des Web 2.0 wirtschaftlich unmöglich gemacht würde.[650] Die datenschutzrechtliche Verantwortlichkeit weist hierbei eine entscheidende Besonderheit auf, die es rechtfertigt, sie von dieser Privilegierung auszunehmen: Um überhaupt als verantwortliche Stelle eingestuft zu werden, muss der Datenverarbeiter eine hinreichende Kontrolle über Zwecke und Mittel der Datenverarbeitung ausüben. Wer derart einzustufen ist, wird in Bezug auf diese Datenverarbeitung grundsätzlich nicht für ausschließlich fremdes Verhalten verschuldensunabhängig in Anspruch genommen, da er ansonsten bereits den Tatbestand der verantwortlichen Stelle nicht erfüllen würde. Die Prüfung, ob ein hinreichender Zurechnungszusammenhang besteht, verlagert sich im Datenschutzrecht mithin in die Frage, ob der Datenverarbeiter eine verantwortliche Stelle ist. Wird dies bejaht, wäre es ein Widerspruch, diese Verantwortlichkeit auf einer späteren Stufe wieder einzuschränken, weil – angeblich – keine hinreichende Kontrolle über den Vorgang der Datenverarbeitung bestand.

In dieser Unterscheidung liegt der Grund, warum eine anlasslose Prüfpflicht hinsichtlich der Datenschutzkonformität der nutzergenerieten Inhaltsdaten für Anbieter sozialer Netzwerke verhältnismäßig ist. Nutzergenerierte, personenbezogene Inhaltsdaten haben für die Anbieter sozialer Netzwerke eine vollkommen andere Bedeutung als beispielsweise für die Anbieter sonstiger Content-Provider wie etwa Verkaufsplattformen oder Blogportale. Bei Anbietern sozialer Netzwerke stehen diese Daten – wie im vorigen Abschnitt gezeigt – in einem untrennbaren wirtschaftlich-funktionellen Zusammenhang zum gesamten Geschäftsmodell.[651] Eine vergleichbare Verknüpfung liegt bei vielen anderen Content-Providern im Regelfall nicht vor. Verkaufsplattformen generieren ihre Einnahmen vor allem über Provisionen bei Verkäufen, sowie gegebenenfalls durch das Anbieten von Werbeflächen.[652] In beiden Fällen sind sie nicht auf die Verarbeitung der Inhaltsdaten ihrer Nutzer angewiesen. Insbesondere der Verkauf der Werbeflächen stellt sich als mehrseitiges Rechtsgeschäft dar, in dem die Diensteanbieter selbst nicht mit personenbezogenen Daten umgehen. Vielmehr stellen sie ihre Werbefläche nur einem anderen werbenden Unternehmen zur Verfügung, welches seinerseits einen Vertrag mit einem auf Nutzerprofile spezialisierten Unternehmen abschließt, um die Werbung nur solchen Nutzern anzeigen zu lassen, die sich hierfür wahrscheinlich interessieren.[653] Ähnliches gilt für Webblogger oder Videoplattformen. Selbst wenn sie

650 Ständige Rechtsprechung des BGH, statt vieler BGH, NJW 2011, 753 (754) Rn. 17 m.w.N.; *Baldus*, in: MüKo-BGB, Bd. 6, § 1004 BGB, Rn. 186 f. m.w.N.; ausführlich zur Unterscheidung negatorischen Eigentumsschutzes und verschuldensabhängiger deliktsrechtlicher Haftung auf Schadensersatz *ders.*, in: MüKo-BGB, Bd. 6, § 1004 BGB, Rn. 41 ff.

651 Hierzu ausführlich oben unter D.I.3.a)aa).

652 *Schapiro*, Unterlassungsansprüche, S. 16; *Arning/Moos*, ZD 2014, 242 (242 f.).

653 Instruktiv hierzu: *Arning/Moos*, ZD 2014, 242 (242 ff.); vgl. auch *ders./ders.*, ZD 2014, 126 (127 f.).

Funktionen anbieten, die es ermöglichen, nutzergenerierte Inhaltsdaten über Dritte zu erheben und zu speichern, wird dies in aller Regel nicht in einer Form mit ihrem Geschäftsmodell verknüpft sein, dass ein untrennbarer wirtschaftlich-funktioneller Zusammenhang besteht. Sie wären daher bereits nicht als datenschutzrechtlich verantwortliche Stelle einzustufen, so dass die hier getroffenen Feststellungen zu den Anbietern sozialer Netzwerke für sie keine Auswirkungen haben.

Dieser Maßstab für die datenschutzrechtliche Verantwortlichkeit findet sich auch bereits in der Entscheidung des BGH zu dem Lehrerbewertungsportal „Spickmich", in welchem der BGH nach Ablehnung der Anwendbarkeit des § 10 TMG eine datenschutzrechtliche Verantwortlichkeit des Plattformbetreibers unproblematisch bejaht.[654] Bewertungsportale leben wie soziale Netzwerke von den nutzergenerierten Inhaltsdaten, mithin den Bewertungen. Zentraler Streitpunkt der Entscheidung ist nur, ob das in § 41 BDSG enthaltene Medienprivileg Anwendung findet – was vom BGH verneint wird – und ob es einen Erlaubnistatbestand für die Datenverarbeitung durch den Plattformbetreiber gibt.[655] Dass es zunächst die Nutzer sind, die die Inhaltsdaten eingeben, die sodann vom Plattformbetreiber gespeichert und weiterverarbeitet werden, wird für die datenschutzrechtliche Verantwortlichkeit für diese Speicherung nicht als bedeutsam eingestuft. Vielmehr sei der Plattformbetreiber als „Herr des Angebots" grundsätzlich verantwortlich bzw. werde es von den Parteien auch gar nicht in Zweifel gezogen, dass der Portalbetreiber selbst personenbezogene Daten speichere, erhebe und übermittle.[656] Dieser Einstufung ist – wenngleich eine nähere Begründung wünschenswert gewesen wäre, inwiefern die Betreiber des Bewertungsportals die Mittel und Zwecke der Datenverarbeitung kontrollieren – im Ergebnis zuzustimmen.

Die datenschutzrechtliche Verantwortlichkeit unabhängig von der Verletzung konkreter Prüfpflichten ist auch keine unverhältnismäßige Belastung für die Anbieter sozialer Netzwerke. Hierbei ist zunächst zu beachten, dass aus der datenschutzrechtlichen Verantwortlichkeit andere Rechtsfolgen erwachsen als aus einer zivilrechtlichen Haftung oder strafrechtlichen Verantwortlichkeit. Während letztere zu Schadensersatzpflichten oder strafrechtlichen Konsequenzen führen können, sind im Falle der datenschutzrechtlichen Verantwortlichkeit primär Betroffenenrechte zu beachten, also insbesondere Benachrichtigungs-, Aufbewahrungs-

654 BGH, NJW 2009, 2888 (2889 f.), Rn. 14 ff. – Spickmich.
655 BGH, NJW 2009, 2888 (2890 f.), Rn. 18 ff. – Spickmich.
656 BGH, NJW 2009, 2888 (2890), Rn.14, 18 – Spickmich; *Kamp*, Personenbewertungsportale, S. 23, 47.

und Löschungspflichten sowie Auskunftsrechte und Unterlassungspflichten.[657] Bußgelder für rechtswidrige Datenverarbeitungen können dagegen nur dann verhängt werden, wenn neben der datenschutzrechtlichen Verantwortlichkeit auch ein aktives Verschulden in Form von Vorsatz oder Fahrlässigkeit hinzutritt, vgl. § 43 Abs. 1 u. 2 BDSG und zukünftig Art. 83 Abs. 2 lit. b) und Abs. 3 DS-GVO. Ähnliches gilt für Schadensersatzansprüche gemäß § 7 BDSG, die ebenfalls nur durchsetzbar sind, sofern sich die verantwortliche Stelle nicht gemäß § 7 S. 2 BDSG durch den Nachweis der Beachtung der gebotenen Sorgfalt exkulpieren kann. Eine ähnliche, wenngleich deutlich strengere Möglichkeit der Exkulpation besteht zukünftig nach Art. 79 Abs. 3 DS-GVO, wenn der für die Verarbeitung Verantwortliche nachweisen kann, in keinerlei Hinsicht für den Umstand verantwortlich zu sein, durch den der Schaden eingetreten ist.

Zwar können die datenschutzrechtlichen Pflichten gegenüber dem Betroffenen, insbesondere die Benachrichtigungspflicht gemäß § 33 Abs. 1 BDSG, über die bloße Pflicht zur Unterlassung gemäß § 1004 BGB analog hinausgehen. Hieraus lässt sich aber nicht der Einwand ableiten, dass eine verschuldensunabhängige datenschutzrechtliche Verantwortlichkeit unverhältnismäßig sei, weil für umfangreichere Pflichten niedrigere Hürden angesetzt würden, indem auf die Verletzung zumutbarer Prüfpflichten oder die positive Kenntnis von der Rechtswidrigkeit verzichtet werde.

Zum einen verkennt eine solche Argumentation den zuvor dargelegten strukturellen Unterschied zwischen zivilrechtlicher Handlungsfreiheit und dem Verbot mit Erlaubnisvorbehalt im Datenschutzrecht. Der Anbieter eines sozialen Netzwerks, der seine Nutzer ermutigt, personenbezogene Inhaltsdaten über Dritte zu erheben und zu übermitteln, um diese sodann für sein eigenes Geschäftsmodell zu nutzen, kann nicht davon ausgehen, dies ohne eine gesetzliche Erlaubnis oder eine Einwilligung eben dieser Betroffenen tun zu dürfen.

Zum anderen ist zu berücksichtigen, dass die datenschutzrechtlichen Pflichten im Rahmen der Verhältnismäßigkeit teleologisch reduziert werden können, um eine Angemessenheit im Einzelfall sicherzustellen. Insbesondere die Benachrichtigungspflicht des § 33 BDSG wird

[657] Freilich könnte es mit nicht unerheblichen Kosten für den Anbieter eines sozialen Netzwerks verbunden sein, eine technische Infrastruktur einzurichten, die die Einhaltung dieser Pflichten sicherstellt. Auch an dieser Stelle gilt indes wieder, dass es nicht Aufgabe des Rechts sein kann, Betroffenenrechte in einem erheblichen Ausmaß zu opfern, um profitable Geschäftsmodelle insbesondere global agierender Datenverarbeitungsunternehmen wie Facebook oder Google nicht zu gefährden. Ein Unternehmen, das sich entschließt, mit den in sozialen Netzwerken generierten Daten Profite zu machen, muss sich daher auch seiner datenschutzrechtlichen Verantwortlichkeit stellen.

beispielsweise dahingehend teleologisch reduziert, dass dem Datenverarbeiter der Name und die Anschrift bzw. zumindest eine Emailadresse des Betroffenen bekannt sein muss, um dieser Pflicht zu unterliegen. Es würde dem Schutzzweck der Norm widersprechen, wenn diese zunächst ermittelt werden müssten – und damit eine weitergehende Datensammlung stattfinden müsste – nur um die Benachrichtigung durchzuführen.[658] Eine Benachrichtigungspflicht wird daher im Regelfall nur gegenüber registrierten Nutzern des sozialen Netzwerks bestehen, nicht aber gegenüber Dritten.[659] Die Norm ist auch dann anzuwenden, wenn die personenbezogenen Daten in anonymisierter Form weitergegeben werden.[660] Es ist indes höchst fraglich, ob die Anbieter sozialer Netzwerke dieser Pflicht aktuell praktisch nachkommen.

Die datenschutzrechtliche Verantwortlichkeit unabhängig von einer Verletzung konkreter Prüfpflichten erweist sich auch als verhältnismäßig, wenn man die legitimen Schutzinteressen der Betroffenen mit dem Aufwand und den geschäftlichen Interessen des Anbieters eines sozialen Netzwerks abwägt. Gerade bei den großen, kommerziellen sozialen Netzwerken, deren gesamtes Geschäftsmodell auf der effizienten Auswertung von Daten beruht, ist davon auszugehen, dass sie über Möglichkeiten verfügen, gespeicherte nutzergenerierte personenbezogene Inhaltsdaten über Dritte im Falle eines Auskunftsverlangens des Betroffenen zu finden und mitzuteilen. Sollten diese wider Erwarten nicht existieren – und diese Daten gleichsam nutzlos und unauffindbar im Nirwana der Server des sozialen Netzwerks gespeichert

658 *Dix*, in: Simitis, BDSG, § 33 Rn. 20 m.w.N.

659 Freilich ist für diese ohnehin fraglich, inwieweit die nutzergenerierten Inhaltsdaten über solche Personen personenbezogen für den Anbieter des sozialen Netzwerks wären. Dies wäre im Einzelfall danach zu bestimmen, ob der Anbieter die nutzergenerierten Inhaltsdaten mit seinem verfügbaren Zusatzwissen einer bestimmten Person zuordnen kann, hierzu bereits ausführlich unter C.III.4.c).

660 *Dix*, in: Simitis, BDSG, § 33 Rn. 26.

sein – ist es technisch zumindest vorstellbar, solche Möglichkeiten beispielsweise durch entsprechende Suchalgorithmen und automatische Indexierungen zu schaffen.[661]

Die datenschutzrechtliche Verantwortlichkeit einzuschränken, weil sie zu erheblichen zusätzlichen Pflichten führen würde[662], würde eine unverhältnismäßige Schutzlosstellung der Betroffenen nach sich ziehen, während der Anbieter wirtschaftlich uneingeschränkt von den Daten profitieren könnte. Wenn nämlich der Anbieter des sozialen Netzwerks nicht zentralisiert datenschutzrechtlich Verantwortlicher und entsprechend Adressat der Auskunfts- und Löschungsrechte wäre, müssten interessierte Betroffene sich bei jedem einzelnen Nutzer, der personenbezogene Daten von ihnen übermittelt haben könnte, hierüber informieren. Dies würde zu einem faktischen Leerlaufen der datenschutzrechtlichen Ansprüche führen.[663] Zudem läge es im Rahmen der Beweislast der Betroffenen nachzuweisen, welche von den gespeicherten Daten zur weiteren Profilbildung verwendet wurden und welche „nur" gespeichert und weiteren Nutzern zum Abruf zur Verfügung gestellt wurden. Einen solchen Beweis werden die Betroffenen aber mangels Einblick in die inneren Verarbeitungsabläufe des Anbieters des sozialen Netzwerks regelmäßig nicht erbringen können.

iv) Zwischenergebnis

Weder die Privilegierungen der §§ 8-10 TMG noch die Grundsätze der Begrenzung der zivilrechtlichen Störerhaftung sind auf die datenschutzrechtliche Verantwortlichkeit zu

---

661 Gerade im Falle von Facebook ist es sehr wahrscheinlich, dass derartige Möglichkeiten existieren, bzw. zumindest daran gearbeitet wird, sie zu erhalten, um eine größtmögliche Auswertung der von Nutzern generierten Inhaltsdaten zu ermöglichen und damit keine „Ressourcen" in Form dieser Daten zu verschwenden. In einer offiziellen Fragestunde am 30.06.2015 antwortete *Marc Zuckerberg*, Gründer und Vorstandsvorsitzender von *Facebook Inc.*, auf die Frage eines Nutzers, in welchen Bereichen der künstlichen Intelligenz Facebook gerade seine Forschung konzentriere: „Most of our AI research is focused on understanding the meaning of what people share. *For example, if you take a photo that has a friend in it, then we should make sure that friend sees it.* (Hervorhebung der Verfasserin) If you take a photo of a dog or write a post about politics, we should understand that so we can show that post and help you connect to people who like dogs and politics. In order to do this really well, our goal is to build AI systems that are better than humans at our primary senses: vision, listening, etc. For vision, we're building systems that can recognize everything that's in an image or a video. This includes people, objects, scenes, etc. These systems need to understand the context of the images and videos as well as whatever is in them. For listening and language, we're focusing on translating speech to text, text between any languages, and also being able to answer any natural language question you ask. This is a pretty basic overview. There's a lot more we're doing and I'm looking forward to sharing more soon." (https://www.facebook.com/zuck/posts/10102213601037571). Es wird mithin ein erheblicher Aufwand darin investiert, nutzergenerierte Inhalte automatisch durch die Software zu verstehen und mit anderen Nutzern gegebenenfalls zu verknüpfen. *Chmelik*, Social Network Sites, S. 86 f. weist darüber hinaus darauf hin, dass die von sozialen Netzwerken vorgenommene Auswahl, welche Inhalte sie Nutzern auf deren Pinnwand oder Timeline präsentiert, voraussetzt, dass die Anbieter diese Informationen zuvor nach inhaltlichen Kriterien sortieren und zuordnen konnten.

662 So im Ergebnis *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 361.

663 So auch *Kauß*, Revisionsbegründung zum BVerwG, Az. 1 C 28.14 vom 02.01.2015, S. 33 ff.; vgl. im Ergebnis auch *Dix*, in: Simits, BDSG, § 35 Rn. 8.

übertragen. § 3 Abs. 7 BDSG und zukünftig Art. 4 Nr. 7 DS-GVO verlangen eine hinreichende Kontrolle über die Zwecke und Mittel der Datenverarbeitung, die, sofern sie vorliegt, eine hinreichende Unmittelbarkeit der Verantwortlichkeit begründet und einer späteren Einschränkung durch eine Statuierung zumutbarer Prüfpflichten entgegensteht. Bei der Verarbeitung von nutzergenerierten Inhaltsdaten durch die Anbieter sozialer Netzwerke – auch in Form der bloßen Erhebung und Speicherung – liegt eine solche Kontrolle vor. Die hieraus resultierende anlasslose datenschutzrechtliche Prüfpflicht für nutzergenerierte, personenbezogene Inhaltsdaten über Dritte ist nicht durch § 7 Abs. 2 TMG ausgeschlossen und stellt in der Abwägung mit den geschützten Betroffenenrechten für die Anbieter von sozialen Netzwerken auch keine unverhältnismäßige Einschränkung dar.

Eine Reduzierung der datenschutzrechtlichen Pflichten ist nur in solchen Fällen denkbar, in welchen die Erfüllung der Pflicht dem Zweck der Pflicht entgegenstünde, beispielsweise im Rahmen von § 33 BDSG bzw. Art. 13 und 14 DS-GVO. Die bloße Unwirtschaftlichkeit der Pflichterfüllung ist dagegen kein Grund für eine Privilegierung der Anbieter sozialer Netzwerke.

Die Erhebung und Verarbeitung nutzergenerierter Inhaltsdaten durch die Anbieter sozialer Netzwerke ist daher nur dann rechtmäßig, wenn diese über eine entsprechende gesetzliche Erlaubnis verfügen oder der Betroffene wirksam eingewilligt hat. Die denkbaren gesetzlichen Erlaubnistatbestände sollen im Folgenden untersucht werden.

cc) Erlaubnistatbestände für die Datenverarbeitung von nutzergenerierten Inhaltsdaten

Die maßgeblichen Erlaubnisvorschriften für die Verarbeitung nutzergenerierter Inhaltsdaten durch nicht-öffentliche Stellen sind bisher die §§ 28, 29 BDSG und zukünftig Art. 6 Abs. 1 DS-GVO.[664] Da es sich bei sozialen Netzwerken als Ganzes nicht um journalistisch-redaktionell aufbereitete Angebote der Presse handelt, sind die Sonderregelungen des Medienprivilegs gemäß § 41 Abs. 1 BDSG entgegen einiger Stimmen in der Literatur[665] nicht anwendbar.[666]

---

664 Instruktiv: *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 356 ff.; Zur Anwendung des BDSG auf Inhaltsdaten bereits ausführlich oben unter C.III.4..

665 Vgl. *Greve/Schärdel*, MMR 2008, 644 (647 f.); *Plog*, CR 2007, 668 (669).

666 BGH, NJW 2009, 2888 (2890), Rn. 19b – Spickmich; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 357; *Dix*, in: Simitis, BDSG, § 41 Rn. 11; vgl. auch *Westphal*, in: Taeger/Gabel, § 41 BDSG, Rn. 24 ff.; *Buchner*, in: Wolff/Brink, § 41 BDSG, Rn. 26 f.; *Wedde*, in: DKWW, § 41 BDSG, Rn. 7; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 75 f.; *Hoidn*, in: Roßnagel (Hrsg.), Europäische DS-GVO, § 4, Rn. 167 ff.

Soweit Nutzer personenbezogene Inhaltsdaten über sich selbst in soziale Netzwerke einstellen, stellt dies für sie keinen Schritt der Datenverarbeitung dar, da sie mit eigenen Daten umgehen.[667] Allerdings nimmt der Anbieter des sozialen Netzwerks aus den oben unter D.I.3.a)aa) dargelegten Gründen eine Erhebung der Daten sowie eine Speicherung gemäß § 3 BDSG bzw. Art. 4 Nr. 2 DS-GVO vor. Diese werden in aller Regel bereits durch eine Einwilligung der Nutzer gemäß §§ 4 Abs. 1 und 4a BDSG bzw. Art. 6 Abs. 1 lit. a) und Art. 7 DS-GVO gedeckt sein, da davon auszugehen ist, dass ein Nutzer, der seine eigenen Daten bewusst in einem sozialen Netzwerk preisgibt, sich auch mit der Erhebung und Speicherung derselben einverstanden erklärt.[668] Eine weitere Verarbeitung durch den Anbieter ist dagegen nur insoweit zulässig, wie dies nach den §§ 28 ff. BDSG, insbesondere einer Interessenabwägung gemäß §§ 28 Abs. 1 S. 1 Nr. 2 und 29 Abs. 1 Nr. 1 BDSG bzw. Art. 6 Abs. 1 lit. f) DS-GVO gestattet ist oder eine explizite hierauf bezogene Einwilligung der Nutzer vorliegt.[669] Dies ist im Einzelfall festzustellen. Hierbei ist insbesondere zu prüfen, ob die Einwilligung hinreichend informiert und bestimmt erfolgte, was nicht zuletzt in Bezug auf die erfolgende Reichweitenanalyse häufig in Frage gestellt werden kann.[670]

Problematisch sind auch hier die nutzergenerierten Inhaltsdaten über Dritte, wenn diese vom Anbieter erhoben, gespeichert und übermittelt werden. Bei solchen kann es sich für den Anbieter als sehr schwierig erweisen, im Einzelfall die gemäß §§ 28 Abs. 1 S. 1 Nr. 2 und 29 Abs. 1 Nr. 1 BDSG bzw. Art. 6 Abs. 1 lit. f) DS-GVO erforderliche Interessenabwägung vorzunehmen.[671] Besondere Schwierigkeiten bereitet die schiere Menge der nutzergenerierten Inhaltsdaten. Wie oben bereits ausgeführt wurde, liegt es indes in der Verantwortung der Anbieter sozialer Netzwerke, z.B. durch Indexierung dieser Daten entsprechende technische Vorkehrungen zu schaffen.[672] Weitere Probleme liegen in dem sehr geringen Einfluss der Anbieter auf die Auswahl der konkret übermittelten Daten, der ihnen allenfalls mittelbar über die Plattformgestaltung zukommt, sowie in dem fehlenden Kontakt zu den Betroffenen, was eine Abschätzung der Auswirkungen der Datenverarbeitung erschwert. Dennoch lässt sich in Bezug auf den zukünftigen Verwendungskontext im konkreten Einzelfall durchaus eine

667 Vgl. *Dammann*, in: Simitis, BDSG, § 3 Rn. 226.
668 Vgl. *Spindler/Nink*, in: Spindler/Schuster, § 4a BDSG Rn. 17.
669 Vgl. *Spindler/Nink*, in: Spindler/Schuster, § 4a BDSG; *Härting*, CR 2011, 169 (172 f.).
670 Zu systematischen Problemen der Bestimmtheit und Informiertheit bei der Einwilligung ausführlich unten unter D.III.2.b).
671 Vgl. *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 361.
672 Vgl. oben unter D.I.3.a)aa).

sinnvolle Interessenabwägung vornehmen und können zumindest verallgemeinerte schutzwürdige Interessen eines Betroffenen ermittelt werden.[673]

Es wird, unter anderem in Anlehnung an die *Spickmich*-Entscheidung des BGH, verbreitet vertreten, dass für die Bereitstellung von Daten durch den Anbieter in sozialen Netzwerken § 29 BDSG anwendbar sei, da die Daten für den Austausch der Nutzer untereinander zur Befriedigung ihres Informationsinteresses erhoben würden.[674] Tatsächlich dürfte dies jedenfalls für kommerzielle soziale Netzwerke deutlich differenzierter zu sehen sein. Die dem *Spickmich*-Urteil zugrunde liegende Bewertungsplattform für Lehrer verfolgte tatsächlich keine eigenen Geschäftszwecke mit den erhobenen Daten, sondern hielt sie nur für eine Übermittlung an Dritte bereit, ohne hierbei erhebliche wirtschaftliche Interessen zu verfolgen.[675] Werbeeinnahmen wurden zwar ebenfalls über die Seite generiert, stellten aber nicht den zentralen Geschäftszweck dar.[676] Dies ist bei kommerziellen sozialen Netzwerken mitnichten der Fall, deren gesamtes Geschäftsmodell auf der Akkumulation und internen Auswertung der generierten Daten aufbaut, um sodann gewinnbringend Werbeanzeigen platzieren zu können. Anders als bei dem Bewertungsportal *Spickmich* ist der Zweck der Datenerhebung damit untrennbar mit der Finanzierung der Webseite durch Werbeeinnahmen verbunden.

Die nutzergenerierten Inhaltsdaten darauf zu reduzieren, dass sie für das Informationsinteresse und die Förderung des Meinungsaustausches zwischen Nutzern erhoben werden, bedeutet die Augen vor der Rolle zu verschließen, die diese für die Generierung weiterer Bestands-, Inhalts- und Nutzungsdaten für das soziale Netzwerke haben.[677] Unabhängig von einer weiteren Verarbeitung der Daten im Rahmen von z.B. einer Profilerstellung, die zweifellos eine neue, für sich rechtfertigungsbedürfte Datenverarbeitung darstellen würde, ist auch die bloße Speicherung und Übermittlung der nutzergenerierten Inhaltsdaten eng mit dem Geschäftszweck der Anbieter sozialer Netzwerke verbunden. Dass insbesondere Facebook dies auch als Teil der Nutzungsvereinbarung und damit des Geschäftszwecks betrachtet, zeigt sich auch an seinen

673 Vgl. BGH, NJW 2009, 2888 (2891), Rn. 26 – Spickmich; *Cebulla*, ZD 2015, 507 (509); instruktiv zur Interessenabwägung: *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 61 ff.

674 *Ehmann*, in: Simitis, BDSG, § 29 Rn. 96 m.w.N.; *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 37 sowie ebenda § 29 BDSG Rn. 13; *Piltz*, CR 2011, 657 (660 f.); a.A. wohl OLG Hamburg, ZD 2011, 138 (139 f.), allerdings konkret nur bezogen auf die Bereitstellung von Daten in Internetforen; *Kremer*, CR 2012, 438 (445).

675 BGH, NJW 2009, 2888 (2891), Rn. 24 – Spickmich.

676 BGH, NJW 2009, 2888 (2891), Rn. 24 – Spickmich.

677 Hierzu bereits ausführlich oben unter C.II.4.b)cc) und D.I.3.a)aa).

Datenrichtlinien, in welchen angegeben ist, dass „alle uns zur Verfügung stehenden Informationen“ verwendet werden, „um unsere Dienste anzubieten und zu unterstützen“.[678]

Angesichts dieser untrennbaren Verknüpfung der Datenspeicherung mit wirtschaftlichen, geschäftlichen Zwecken ist daher im Regelfall § 28 BDSG als maßgebliche Erlaubnisnorm für die Anbieter sozialer Netzwerke heranzuziehen.[679] Das Vorliegen der Voraussetzungen, insbesondere die nach § 28 Abs. 1 Nr. 2 BDSG erforderliche Interessenabwägung, ist im Einzelfall festzustellen.

Sollten personenbezogene Daten netzwerköffentlich zur Verfügung gestellt worden sein, kommen darüber hinaus die §§ 28 Abs. 1 Nr. 3, 29 Abs. 1 Nr. 2 BDSG als Erlaubnisnorm in Betracht. Allgemein zugänglich sind Daten, „die sich sowohl ihrer Zielsetzung als auch ihrer Publikationsform nach dazu eignen, einem *individuell nicht bestimmbaren Personenkreis* Informationen zu vermitteln.“[680] Dies trifft grundsätzlich auf Daten zu, die innerhalb eines sozialen Netzwerks öffentlich einsehbar sind, also ohne eine bestätigte Kontaktanfrage.[681] Zwar ist eine Registrierung im Netzwerk erforderlich, um auf die Daten zuzugreifen. Da hierbei aber keine wirkliche Kontrolle erfolgt und die Registrierung regelmäßig kostenlos ist, stellt dies keine besondere Zugangshürde dar. Freilich kommt es zu Problemen mit der Wahrung der informationellen Selbstbestimmung, wenn die Betroffenen, deren Daten von anderen Nutzern derart veröffentlicht werden, mit dieser Veröffentlichung nicht einverstanden waren.[682] Zudem können die Daten sehr leicht in einem anderen Kontext verarbeitet werden als sie ursprünglich übermittelt und veröffentlicht wurden.[683] Umso wichtiger sind daher effektive Informationsansprüche und Widerspruchsrechte der Betroffenen, um derartige Eingriffe zu

678 https://www.facebook.com/privacy/explanation (Stand 29. September 2016).

679 Vgl. auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 91 f.

680 *Simitis*, in: Simitis, BDSG, § 28 Rn. 151 m.w.N.

681 *Taeger*, in: Taeger/Gabel, § 28 Rn. 83; *Kramer*, in: Auernhammer, § 28 BDSG, Rn. 20; *Plath*, in: Plath, § 28 BDSG, Rn. 76; a.A. *Wolff*, in: Wolff/Brink, § 28 BDSG, Rn. 83; *Wedde*, in: DKWW, § 28 BDSG, Rn. 58.

682 Vgl. auch *Gola/Schomerus*, § 28 BDSG, Rn. 31 f.; *Wedde*, in: DKWW, § 28 BDSG, Rn. 58 verneint in diesem Fall eine allgemeine Zugänglichkeit der Daten, um die informationelle Selbstbestimmung der Betroffenen zu schützen. Dies überzeugt allerdings nicht, da es zu massiver Rechtsunsicherheit führen den Datenverarbeiter führen würde, der das Vorliegen dieses Einverständnis‘ des Betroffenen regelmäßig niemals überprüfen könnte.

683 *Simitis*, in: Simitis, BDSG, § 28 Rn. 150 stellt zutreffend fest, dass die Wertungen der Informationsfreiheit gemäß Art. 5 Abs. 1 S. 1 GG, welche der Regelung des § 28 Abs. 1 Nr. 3 BDSG zugrunde liegen, nicht ohne Weiteres auf eine Weiterverarbeitung etwa zu Werbezwecken übertragen werden können. Eine Beschränkung der Weiterverarbeitungsfreiheit beispielsweise durch Normierung von Betroffenenrechten ist daher nicht nur verfassungsrechtlich zulässig, sondern kann vielmehr sogar zur Wahrung der informationellen Selbstbestimmung geboten sein. Insbesondere im Falle von nutzergenerierten Inhaltsdaten über Dritte ist daher eine eher restriktive Handhabung der Erlaubnisvorschrift des § 28 Abs. 1 Nr. 3 BDSG, bzw. § 29 Abs. 1 Nr. 2 BDSG angezeigt.

unterbinden. Zudem kann auch hier die Interessenabwägung im Einzelfall der Zulässigkeit der Verarbeitung entgegenstehen.[684]

Eine Einwilligung dürfte dagegen als Rechtsgrundlage im Fall nutzergenerierter Inhaltsdaten über Dritte regelmäßig ausscheiden, da die Betroffenen im Zeitpunkt der Erhebung, Speicherung und Übermittlung oft gar nicht von dieser wissen.[685]

Darüber hinaus kann sich ein grundlegendes Problem aus dem Grundsatz der Direkterhebung gemäß § 4 Abs. 2 S. 1 BDSG ergeben, welches bisher nur vereinzelt in Bezug auf soziale Netzwerke diskutiert wird.[686] Gemäß der Regelung sind Daten prinzipiell direkt bei dem Betroffenen zu erheben. Wie indes bereits festgestellt wurde, ist der Betroffene häufig im Zeitpunkt des Einstellens der Daten in ein soziales Netzwerk nicht über diesen Vorgang informiert. Eine Direkterhebung beim Betroffenen liegt damit regelmäßig nicht vor.[687]

Wiewohl der Grundsatz der Direkterhebung einen wichtigen Baustein zur Gewährleistung der informationellen Selbstbestimmung darstellt, wirkt er in Zeiten ubiquitärer Datenverarbeitung etwas antiquiert. Hierauf reagiert die DS-GVO, die in Art. 14 DS-GVO lediglich eine Informationspflicht des für die Datenverarbeitung Verantwortlichen statuiert, soweit dieser Daten verarbeitet, welche nicht bei dem Betroffenen erhoben wurden.[688] Der Grundsatz der Direkterhebung wird damit implizit aufgegeben, so dass die mit ihm verbundenen Probleme in sozialen Netzwerken mit Anwendbarkeit der DS-GVO entfallen werden.

Auch in der bisherigen Rechtslage kann die Erhebung von nutzergenerierten, personenbezogenen Inhaltsdaten über Dritte allerdings unter den Voraussetzungen des § 4 Abs. 2 S. 2 BDSG zulässig sein. In Betracht kommen insbesondere die Ausnahmen der Nr. 2 lit.a) und Nr. 2 lit.b), wonach Daten ohne Mitwirkung des Betroffenen erhoben werden dürfen, wenn dies entweder nach dem Geschäftszweck der verantwortlichen Stelle erforderlich ist oder eine Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand darstellen würde.[689]

---

684 *Gola/Schomerus*, § 28 BDSG, Rn. 31 f.; Überblick zur Interessenabwägung, insbesondere in Bezug auf Personenbewertungsportale bei *Taeger*, in: Taeger/Gabel, § 28 Rn. 103 ff.

685 Ausführlich: *Buchner*, Facebook zwischen BDSG und UWG, in: FS Köhler, S. 53 ff.; vgl. auch *Cebulla*, ZD 2015, 507 (510); *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 91 f.

686 Kurz hierzu *Jandt/Roßnagel*, ZD 2011, 160 (162); *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 92; vgl. allerdings zum Umgang mit Kollateraldaten in Bezug auf vernetzte Kraftfahrzeuge *Cebulla*, ZD 2015, 507 (508 ff.); ebenfalls in diesem Kontext als Problem angedeutet von *Hornung/Goeble*, CR 2015, 265 (272).

687 *Jandt/Roßnagel*, ZD 2011, 160 (162); *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 92.

688 *Cebulla*, ZD 2015, 507 (511); für eine Beibehaltung des Direkterhebungsgrundsatzes plädieren dagegen *Roßnagel/Richter/Nebel*, ZD 2013, 103 (105).

689 So allgemein für den Umgang mit Kollateraldaten bereits *Cebulla*, ZD 2015, 507 (510).

Angesichts der Funktionsweise sozialer Netzwerke ist es durchaus nicht fernliegend, dass dies bei nutzergenerierten Inhaltsdaten über Dritte regelmäßig zutrifft.[690] Freilich bedeutet eine solche Auslegung aber auch eine faktische Aufhebung des Ausnahmecharakters von § 4 Abs. 2 S. 2 BDSG. Inwieweit die Datenverarbeitung zulässig ist, ist daher bis zur Anwendbarkeit der DS-GVO stets im konkreten Einzelfall zu klären.

dd) Zwischenergebnis: Datenschutzrechtliche Verantwortlichkeit der Anbieter sozialer Netzwerke

Anbieter sozialer Netzwerke, die nutzergenerierte Inhaltsdaten wirtschaftlich verwerten, sind vollumfänglich datenschutzrechtlich verantwortlich für deren Erhebung und Speicherung, unabhängig von einer konkreten Weiterverarbeitung eines individuellen Datums.[691] Sie unterliegen entsprechend einer anlasslosen Prüfpflicht, ob insbesondere die nutzergenerierten personenbezogenen Daten Dritter datenschutzrechtlich zulässig verarbeitet werden. Die Haftungsprivilegierungen der §§ 8-10 TMG, sowie die Regelungen zur zivilrechtlichen Störerhaftung sind nicht übertragbar. Entsprechend muss für jede Erhebung, Speicherung und weitere Verarbeitung nutzergenerierter Inhaltsdaten eine gesetzliche Erlaubnis oder eine wirksame Einwilligung des Betroffenen vorliegen.

Die Anbieter sind zudem Verpflichtete der Betroffenenrechte, insb. des Auskunftsrechts gemäß § 34 BDSG (Art. 15 DS-GVO) sowie des Berichtigungs- und Löschungsanspruchs gemäß § 35 BDSG (Art. 16 und 17 DS-GVO) und der Benachrichtigungspflicht über gespeicherte personenbezogene Daten gemäß § 33 BDSG (Art. 13 und 14 DS-GVO), mit den zuvor dargelegten teleologischen Einschränkungen.[692] Sollte es soziale Netzwerke geben, deren Anbieter öffentliche Stellen sind – was derzeit nicht ersichtlich ist – wären diese entsprechend nach den §§ 19 ff. BDSG gegenüber den Betroffenen verpflichtet. Eine besondere Erweiterung der datenschutzrechtlichen Pflichten könnte sich aus dem neu geschaffenen Recht auf Datenportabilität gemäß Art. 20 DS-GVO ergeben; dies hängt insbesondere davon ab, inwieweit sich dieser Vorschrift auch eine Interoperabilitätsvorgabe entnehmen lässt.[693]

Darüber hinaus sind die Anbieter sozialer Netzwerke als Diensteanbieter i.S.v. § 2 Nr. 1 TMG auch die Adressaten datenschutzrechtlicher Pflichten nach den §§ 12 ff. TMG, soweit sie Bestands- und Nutzungsdaten verarbeiten. Aufgrund des hier gesetzten Fokus auf

690 a.A. *Jandt/Roßnagel*, ZD 2011, 160 (162).
691 Vgl. auch *Piltz*, Soziale Netzwerke, S. 91; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 83 f. teilweise zustimmend *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 355 ff.
692 Vgl. oben unter D.I.3.a)bb)iii)(2).
693 Hierzu ausführlich unten unter D.III.3.a)bb)iii).

nutzergenerierte Inhaltsdaten wurde auf diese Aspekte indes nicht vertieft eingegangen. Einzig die Pflicht zur Ermöglichung einer anonymen oder jedenfalls pseudonymen Nutzung, welche in einem Spannungsverhältnis zwischen dem Persönlichkeitsschutz und den Möglichkeiten der Rechtsverfolgung steht, soll gesondert unter D.II. näher betrachtet werden.

b) Verantwortlichkeit der Nutzer

Anders als im klassischen dichtomen Ansatz des Datenschutzrechts vorgesehen ermöglichen das Internet im Allgemeinen und soziale Netzwerke im Speziellen auch privaten Nutzern, mit einem Publikum unbestimmter Größe zu kommunizieren und Informationen zu verbreiten. Nutzer von Diensteangeboten werden selbst zu potentiellen Datenverarbeitern, indem sie im Zuge der privaten oder geschäftlichen Nutzung Daten über Dritte erheben, speichern, übermitteln oder verknüpfen.[694] Hiermit stellt sich die Frage nach der datenschutzrechtlichen Verantwortlichkeit von Nutzern in Abgrenzung zu anderen Akteuren im digitalen Kontext.

Speziell in Bezug auf soziale Netzwerke teilt sich die Diskussion um die Verantwortlichkeit der Nutzer in drei Fragestellungen. Zunächst ist zu klären, inwieweit die Anwendbarkeit des Datenschutzrechts und damit auch eine mögliche Verantwortlichkeit grundsätzlich durch das sogenannte „Haushaltsprivileg“ des § 1 Abs. 2 Nr. 3 BDSG bzw. Art. 2 Abs. 2 lit. c) DS-GVO ausgeschlossen ist. Anschließend stellt sich die Frage, ob das Einstellen von Inhaltsdaten durch die Nutzer eine Form der Datenverarbeitung darstellt, die eine datenschutzrechtliche Verantwortlichkeit begründet. In jüngster Zeit ist zudem eine Kontroverse darüber entstanden, inwieweit Nutzer von sozialen Netzwerken (und anderen Onlinediensten) sogar selbst als Diensteanbieter im Sinne von § 2 Nr. 1 TMG zu qualifizieren sind und entsprechend u.a. Impressumspflichten nach § 5 Abs. 1 TMG unterliegen.[695]

Als Sonderfall der Verantwortlichkeit von Nutzern ist die Verantwortlichkeit von „Fanpage“-Anbietern für die Verarbeitung von Bestands- und Nutzungsdaten zu sehen. Dies soll in einem gesonderten Kapitel im Anschluss untersucht werden.

---

694 Dieses Problem benennt auch bereits *Spindler*, GRUR-Beilage 2014, 101 (104); vgl. auch *Sandfuchs*, Privatheit wider Willen, S. 43 f.

695 *Lorenz*, VuR 2014, S. 83 (84 f.); *Richter*, MMR 2014, S. 517 ff.; *Pießkalla*, ZUM 2014, S. 368 (370 f.).; OLG Düsseldorf, K&R 2013, S. 594 ff., m. Anm. *Schönewald*; *Schröder*, WRP 2013, S. 1225 ff.; hierzu ausführlich unten unter D.II.1.

aa) Anwendbarkeit des „Haushaltsprivilegs" gemäß § 1 Abs. 2 Nr. 3 BDSG bzw. Art. 2 Abs. 2 lit. c) DS-GVO

Das „Haushaltsprivileg" schließt Datenverarbeitungen, die von natürlichen Personen „ausschließlich für persönliche oder familiäre Tätigkeiten" vorgenommen werden, vom Anwendungsbereich des Datenschutzrechts aus. Die Regelung existierte bisher in § 1 Abs. 2 Nr. 3 BDSG[696], basierend auf Art. 3 Abs. 2 DSRL, und wird unverändert in Art. 2 Abs. 2 lit. c) DS-GVO übernommen. Angesichts der doch erheblichen Beeinträchtigungen, die für die Rechte Betroffener aus privater Datenverarbeitung erfolgen können, ist diese Zementierung der bisherigen, undifferenzierten Rechtslage sehr bedauerlich.[697]

Von umso größerer Bedeutung ist es, detailliert zu untersuchen, welche Tätigkeiten von dem Haushaltsprivileg erfasst sind. Speziell in sozialen Netzwerken stellt sich hierbei das Problem, dass jedenfalls bei einer rein privaten Nutzung von der subjektiven Zwecksetzung her unzweifelhaft eine persönliche Tätigkeit vorliegt. Zu klären ist aber, ob angesichts des hiermit verbundenen erheblichen Verbreitungspotentials von Informationen und entsprechenden Risiken für die informationelle Selbstbestimmung Betroffener tatsächlich allein auf diese (ggf. verobjektivierte) subjektive Zwecksetzung abzustellen ist, mit der Konsequenz einer vollständigen Nichtanwendbarkeit des Datenschutzrechts.

i) Die gesetzliche Regelung des Haushaltsprivilegs

Ausgangspunkt der Analyse muss nunmehr der Erwägungsgrund 18 DS-GVO sein, welcher seit dem Ratsentwurf vom 15. Juni 2015[698] die „Nutzung sozialer Netze" als ein mögliches Beispiel für eine persönliche oder familiäre Tätigkeit auflistet, zusammen mit dem „Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen", sowie „Online-Tätigkeiten im Rahmen solcher Tätigkeiten". Anders als die deutsche Fassung spricht die englische Fassung etwas abstrakter von „social networking". Man könnte dies als eine rein „offline" geprägte Formulierung interpretieren, angesichts der Tatsache, dass „Online-Tätigkeiten" separat

696 Dieser Ausschluss wird wiederholt in § 27 Abs. 1 Nr. 2 BDSG für den Anwendungsbereich des dritten Abschnitts über Datenverarbeitung durch nicht-öffentliche Stellen. Zudem sind – anders als im Bereich der Datenverarbeitung durch öffentliche Stellen – im nicht-öffentlichen Bereich grundsätzlich nur Verarbeitungen personenbezogener Daten einbezogen, wenn diese durch EDV-Anlagen vorgenommen werden oder einen Bezug zu einer Datei aufweisen bzw. offensichtlich aus einer automatisierten Verarbeitung entnommen wurden, §§ 1 Abs. 2 Nr. 3, 27 Abs. 2 BDSG. Das Schutzniveau liegt damit deutlich niedriger als im Bereich der Datenverarbeitung durch öffentliche Stellen, bei denen jede Form der Verarbeitung personenbezogener Datenverarbeitung erfasst ist. *Dammann*, in: Simitis, BDSG, § 1 Rn. 137 spricht gar von einer „gravierende[n] Absenkung des Schutzniveaus".

697 So auch *Roßnagel/Nebel/Richter*, ZD 2015, 455 (456); vgl. auch *ders./dies./ders.*, ZD 2013, 103 (104).

698 *Rat der Europäischen Union*, Dok. Nr. 9565/15.

hiervon aufgezählt wird. Sollte sie indes (auch) die umfassende Nutzung sozialer Netzwerke im Sinne dieser Arbeit bezeichnen, so verkennt dies in eklatanter Weise die hiermit verbundenen Risiken für andere Betroffene und widerspricht – wie im Folgenden zu zeigen sein wird – der dem Haushaltsprivileg seit jeher zugrunde liegenden Ratio. In Bezug auf die sonstigen Online-Tätigkeiten wäre die Klarstellung zudem offensichtlich tautologisch.

Der Gesetzgeber bezweckt mit dem Haushaltsprivileg die Ermöglichung einer Datenverarbeitung im Bereich persönlicher Lebensführung, beispielsweise in privaten (digitalen) Fotoalben oder Adressbüchern mit ggf. zusätzlichen Angaben über Hobbys und anderen Vorlieben der betroffenen Personen.[699] Das Interesse an einer entsprechenden privaten Datenverarbeitung wird als ebenso schutzwürdig anerkannt wie das Interesse an informationeller Selbstbestimmung des Betroffenen, unabhängig davon, wie intensiv dessen Belange hiervon berührt werden. Auch im Falle von schweren Rechtsverletzungen können sich daher zwar Abwehrrechte ergeben, etwa aus §§ 823 Abs. 1 und 1004 BGB, aber keine datenschutzrechtlichen Ansprüche.[700]

Die traditionelle Abgrenzung der persönlichen Sphäre erfolgt gegenüber einer beruflichen, geschäftlichen oder gewerblichen Sphäre und wird so auch in Erwägungsgrund 18 DS-GVO getroffen. Es ist nach der Verkehrsanschauung zu differenzieren, ob eine Datenverarbeitung zu typisch familiären Zwecken erfolgt wie etwa Freizeit, Liebhabereien, Privatreisen, privater Konsum, Sport oder Unterhaltung.[701] Als beruflich oder gewerblich ist demgegenüber jedenfalls alles zu verstehen, was der Gewinnerzielung oder der Sicherung eines Lebensunterhalts dient, „auch wenn sie im privaten Rahmen, also etwa vom Wohnzimmer aus, ausgeübt werden“.[702] Historisch ist allerdings ein Wandel zu beobachten, der dem Merkmal der Gewinnerzielungsabsicht und dem beruflichen oder gewerblichen Kontext einen immer geringeren Stellenwert zukommen lässt, zugunsten einer qualitativen Abgrenzung anhand der Zwecksetzung und Auswirkung der Datenverarbeitung. National lässt sich dies an der aktuellen negativen Abgrenzung des § 1 Abs. 2 Nr. 3 BDSG zeigen: Bis zur Novelle im Jahr 2001[703] bestimmte das BDSG noch positiv, dass das Datenschutzrecht nur anwendbar sei, wenn Daten

699 *Dammann*, in: Simitis, BDSG, § 1 Rn. 149; *Gusy*, in: Wolff/Brink, § 1 BDSG, Rn. 75; *Wedde*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 4.3, Rn. 36.
700 *Dammann*, in: Simitis, BDSG, § 1 Rn. 149.
701 *Dammann*, in: Simitis, BDSG, § 1 Rn. 151; *Schmidt*, in: Taeger/Gabel, § 1 BDSG, Rn. 31; *Plath*, in: Plath, § 1 BDSG, Rn. 31; vgl. auch *Wedde*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 4.3, Rn. 36; *Jandt/Roßnagel*, ZD 2011, 160 (162).
702 *Dammann*, in: Simitis, BDSG, § 1 Rn. 151; *Plath*, in: Plath, § 1 BDSG, Rn. 32.
703 BGBl. I 2001, S. 904 (905).

„geschäftsmäßig oder für berufliche oder gewerbliche Zwecke“ verarbeitet oder genutzt werden.[704] Dies diente ausweislich der Gesetzesbegründung der Anpassung an die Regelungen der wenige Jahre zuvor verabschiedeten DSRL, konkret Art. 3 Abs. 2 DSRL.[705] Auch der *LIBE*-Entwurf des Parlaments[706] strich das Kriterium der fehlenden Gewinnerzielungsabsicht und stellte stattdessen in Art. 2 Abs. 2 lit.d) DS-GVO-E a.F. darauf ab, ob vernünftigerweise erwartet werden könne, dass die veröffentlichten Daten nur einer begrenzten Zahl von Personen zugänglich gemacht würden.

Es bestand und besteht somit seit jeher sowohl auf nationaler als auch auf europäischer Ebene ein Konsens, jedenfalls berufliche und geschäftliche Datenverarbeitungen stets der Anwendbarkeit des Datenschutzrechts zu unterwerfen. Diese Abgrenzung trifft auch Erwägungsgrund 18 DS-GVO, wenngleich – worauf sogleich zurückzukommen sein wird – das durch den *LIBE*-Entwurf eingefügte Kriterium der zu erwartenden Verbreitung bedauerlicherweise nicht übernommen wurde. Es gilt daher wie auch bisher, dass eine Anwendung des Haushaltsprivilegs bei der Nutzung sozialer Netzwerke jedenfalls dann nicht in Betracht kommt, wenn das Nutzerprofil und die mit ihm vorgenommene Datenverarbeitung auch nur teilweise der beruflichen Selbstvermarktung dient.[707] Dies wird regelmäßig bei Profilen in sozialen Netzwerken der Fall sein, die bereits grundsätzlich auf eine berufliche Sphäre ausgerichtet sind, wie etwa XING oder LinkedIn.[708] Aber auch in allen anderen sozialen Netzwerken besteht grundsätzlich die Möglichkeit, in seinem Profil Bewerbungen zu veröffentlichen, Dienstleistungen anzubieten oder Werbung für Angebote Dritter zu machen.[709] Soweit dies geschieht, ist nicht mehr von einer ausschließlich persönlichen oder familiären Tätigkeit auszugehen.

Problematisch ist hingegen, ob darüber hinaus auch die rein private Nutzung sozialer Netzwerke tatsächlich mit den traditionellen erfassten Tätigkeiten und den anderen Beispielen in Erwägungsgrund 18 DS-GVO vergleichbar ist und ob sie daher dem Haushaltsprivileg

---

704 Vgl. auch *Dammann*, in: Simitis, BDSG, § 1 Rn. 147; *von Lewinsky*, in: Auernhammer, § 1 BDSG, Rn. 17.

705 BT-Drs. 14/4329, S. 27, 31; vgl. auch *von Lewinsky*, in: Auernhammer, § 1 BDSG, Rn. 17; *Gusy*, in: Wolff/Brink, § 1 BDSG, Rn. 75.

706 *EU-Parlament*, P7_TA-PROV(2014)0212.

707 *Simitis*, in: Simitis, BDSG, § 27 Rn. 47; *Plath*, in: Plath, § 1 BDSG, Rn. 33; *Piltz*, Soziale Netzwerke, S. 94, 97; *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 134; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 349; *Ders./Dies.*, ZD 2011, 160 (162); Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 12; vgl. auch *Schmidt*, in: Taeger/Gabel, § 1 BDSG, Rn. 29.

708 *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 134; *Piltz/Trinkl*, in: Hoeren/Bensinger, Kap. 13, Rn. 143; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 349.

709 *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 134; *Piltz/Trinkl*, in: Hoeren/Bensinger, Kap. 13, Rn. 144; vgl. auch unten unter D.I.3.b)cc).

unterfallen sollte. Falls dies bejaht werden sollte, stellt sich zudem die Frage, wie eine konkrete Abgrenzung gestaltet werden kann. Wie im Folgenden zu zeigen ist, sind die maßgeblichen Gesichtspunkte hierbei zum einen das Verbreitungspotential von Informationen in sozialen Netzwerken in Verbindung mit den strukturellen Besonderheiten der Datenverarbeitung in diesen, zum anderen die begrenzten Herrschafts- und Kontrollmöglichkeiten des Nutzers im Rahmen der Nutzung.

ii) Soziale Netzwerke, die Sphärentheorie und der Adressatenkreis

Das Verbreitungspotential von Daten, die in sozialen Netzwerken eingestellt werden, geht weit über das hinaus, was noch vor wenigen Jahren im Rahmen einer persönlichen oder familiären Tätigkeit möglich gewesen wäre. Es ist nur sehr begrenzt vergleichbar mit einem privaten Fotoalbum oder persönlichen Adressbuch, da der potentielle Adressatenkreis und die Möglichkeiten der Rekombination erheblich größer sind. Zur Sicherstellung eines effektiven Datenschutzes ist daher über die klassische Abgrenzung zwischen einer beruflichen oder privaten Sphäre hinaus auch nach dem potentiellen Adressaten- oder Empfängerkreis abzugrenzen, um eine ausschließlich persönliche oder familiäre Tätigkeit zu bestimmen. Dies bedingt natürlich die sogleich zu beantwortende Frage, bei welchen Empfängerkreisen eine Grenze zu ziehen wäre.

Um den Begriff der privaten Sphäre besser zu verstehen, bietet sich ein Rückgriff auf die Dogmatik des allgemeinen Persönlichkeitsrechts an, welches zwischen der Privatsphäre und der öffentlichen Sozialsphäre trennt.[710] Hierbei ist natürlich anzuerkennen, dass das Sphärenmodell im digitalen Informationskontext schnell an seine Grenzen stößt, indem die physische Trennung der einzelnen Sphären aufgehoben ist und eine starke Durchmischung stattfindet: Die Privatheit einer Information oder einer Handlung wird häufig ganz überwiegend durch die subjektive Einstellung und den Verwendungszweck bestimmt.[711] Eben dies wird auch zurecht als Kernbestandteil der informationellen Selbstbestimmung benannt, welche

[710] So auch *Chmelik*, Social Network Sites, S. 228 ff.

[711] *Eichenhofer*, Der Staat (55) 2016, 41 (49 ff.) m.w.N. geht sogar noch einen Schritt weiter und konstatiert, dass eine Datenübertragung im Internet weitgehend unabhängig von dem ursprünglichen Verwendungszusammenhang stattfinde. Privatheit im Internet solle daher generell nicht mehr anhand der Sphärentheorie oder der informationellen Selbstbestimmung bestimmt werden, sondern es sei als Frage des Vertrauensschutzes zu konzipieren. Maßgeblich solle nicht sein, ob der Einzelne tatsächlich Kontrolle über die Verbreitung eines Datums habe, sondern ob er nach den bestehenden Datenschutzregelungen berechtigterweise darauf vertrauen dürfe, dass ein Datum nicht gegen seinen Willen verbreitet werde. Wiewohl in der Problemanalyse zutreffend, gibt diese Konzeption freilich keine normativen Antworten darauf, wo die Grenzen durch das Datenschutzrecht zu ziehen wären.

entsprechend nicht auf die Sphärentheorie zurückgreift.[712] Trotz dieser berechtigten Kritik kann das Sphärenmodell aber dort weiter seine dogmatisch ordnende Funktion erfüllen, wo Konstellationen in einem logischen Sinne klar einer Sphäre zugeordnet werden können.[713] Anstatt auf die überkommenen engen Grenzen einer rein physischen Differenzierung kommt es dabei insbesondere auf die soziale Zugänglichkeit der Information oder der Handlung an, sowie eine Bewertung der damit verbundenen Vertraulichkeitserwartungen.[714]

Soweit die Bestimmungen der DS-GVO auszulegen sind, versteht es sich von selbst, dass diese nicht unmittelbar anhand nationaler Grundrechte konkretisiert werden können. Vielmehr ist auf die Art. 7 und 8 GrCH abzustellen, welche die Rechte auf Achtung des Privatlebens und des Schutzes der personenbezogenen Daten normieren. Tatsächlich bestehen aber weitgehende Übereinstimmungen zum allgemeinen Persönlichkeitsrecht und dem Recht auf informationelle Selbstbestimmung.[715] Dies gilt umso mehr seit dem *Google-Urteil* des EuGH, in welchem dieser implizit eine mittelbare Drittwirkung statuierte, indem er ein „Recht auf Vergessenwerden" gegenüber dem privaten Internetsuchmaschinenbetreiber Google anerkannte und dies mit einer Auslegung der DSRL im Lichte der Art. 7 und 8 GrCH begründete.[716] Angesichts dieser Vergleichbarkeit soll im Weiteren vornehmlich – dem generellen Schwerpunkt dieser Arbeit folgend – begrifflich auf die nationale Grundrechtsterminologie abgestellt werden und nur zu Klarstellungszwecken und bei Abweichungen auf die Grundrechtecharta verwiesen werden.

Mit dem Abgrenzungskriterium der öffentlichen Sphäre kann man die Frage nach der Privatheit zumindest für den denkbar weitesten Empfängerkreis, nämlich alle Nutzer im Internet, relativ eindeutig beantworten: Wenn die übermittelten Daten durch die Privatsphäre-Einstellungen des

712 *Simitis*, in: Simitis, BDSG, § 1 Rn. 65 ff.; *Nebel*, ZD 2015, 517 (518 f.); *Geminn/Roßnagel*, JZ 2015, 703 (706); vgl. auch *Greve*, Drittwirkung, in: FS Kloepfer, S. 6; *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 174.

713 *v. Lewinsky*, Matrix des Datenschutzes, S. 40, 82 f.; vgl. auch *Buchholtz*, AöR 2015, 121 (143 f.); *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 25 f.

714 Ausführlich: *Albers*, DVBl. 2010, 1061 (1065 ff.); *Buchholtz*, AöR 2015, 121 (146 ff.); *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 25 f., 40 ff.; *Chmelik*, Social Network Sites, S. 228 ff.; dies übersieht *Eichenhofer*, Der Staat (55) 2016, 41 (49 f.), der das Konzept der informationellen Selbstbestimmung insofern als „nicht mehr zeitgemäß" bezeichnet.

715 *Augsberg*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 7 Rn. 5, Art. 8 Rn. 6 GrCH; vgl. auch ausführlich *Eichenhofer*, Der Staat (55) 2016, 41 (55 ff.).

716 EuGH, *Google Spain*, Rs. C-131/12, Rn. 38 = JZ 2014, 1009 (1012); *Skouris*, NVwZ 2016, 1359 (1361); *Boehme/Neßler*, NVwZ 2014, 825 (827 f.); *Augsberg*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 8 Rn. 10 GrCH; *Eichenhofer*, Der Staat (55) 2016, 41 (63 f.); vgl. auch *Greve*, Drittwirkung, in: FS Kloepfer, S. 676 f.

Profils im gesamten Internet zugänglich und sichtbar sind[717], wäre es lebensfremd, dies als Handlung im persönlichen und familiären Kreis einzustufen, da es sich um eine Übermittlung der Daten in die (digitale) Öffentlichkeit handelt. Jedenfalls wenn Nutzer Inhaltsdaten derart an soziale Netzwerke übermitteln, dass diese im gesamten Internet ohne Überwindung weiterer Zugangsschranken abrufbar sind, können sie sich daher nicht auf die Privilegierung des § 1 Abs. 2 Nr. 3 BDSG bzw. zukünftig Art. 2 lit. c) DS-GVO berufen.[718]

Soweit die Sichtbarkeit der Inhalte auf andere Nutzer im sozialen Netzwerk beschränkt ist, wird dagegen verbreitet die Anwendbarkeit des Haushaltsprivilegs bejaht, wenn die Nutzer mit der Übermittlung persönliche und keine beruflichen Zwecke verfolgen.[719] Eine (numerische) Begrenzung des Adressatenkreises wird als willkürlich abgelehnt[720], so dass im Falle von Facebook bis zu 1,6 Milliarden andere Nutzer Zugriff auf die Daten haben könnten. Eine engere Variante hiervon ist, die Anwendbarkeit des Haushaltsprivilegs zuzulassen, wenn es sich um Freunde „im hergebrachten Sinn des Wortes“[721] handelt, wobei die entsprechenden Autoren eine Erklärung schuldig bleiben, wie dies rechtssicher festzustellen sein soll, insbesondere für Betroffene, die gegebenenfalls ihre Rechte gegen andere Nutzer geltend machen wollen.

Das Vorliegen einer persönlichen und familiären Tätigkeit im Ergebnis ausschließlich nach der (objektivierten) Zwecksetzung des Nutzers zu bestimmen, greift indes zu kurz und ist abzulehnen.[722] In diesem Sinne hat auch der EuGH bereits zutreffend entschieden, dass die Anbringung einer Videoüberwachung an einem privaten Eigenheim, welche den öffentlichen

---

717 Bei Facebook ist dies beispielsweise möglich durch die Wahl der Privatsphäre-Einstellung „Öffentlich“, mit welcher alle derart freigegeben Beitrage im eigenen Profil für jeden innerhalb und außerhalb von Facebook sichtbar sind, https://www.facebook.com/help/1090831264320592/?helpref=hc_fnav unter „Was sind öffentliche Informationen?“.

718 Vgl. EuGH, *Lindqvist*, Rs. C-101/01, Rn. 47 = EuR 2004, 291 (299); so auch *Piltz*, Soziale Netzwerke, S. 97; *Ders./Trinkl*, in: Hoeren/Bensinger, Kap. 13, Rn. 144; *Maisch*, Informationelle Selbstbestimmung, S. 202 f.; *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 135; *ders./Hoffmann*, JZ 2013, 163 (168); *Dammann*, in: Simitis, BDSG, § 1 Rn. 151; *Jandt/Roßnagel*, ZD 2011, 160 (162); Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 12; *Kamp*, Personenbewertungsportale, S. 41 f.; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 76; *Schantz*, NJW 2016, 1841 (1843); vgl. auch *Dix*, in: Simitis, BDSG, § 35 Rn. 8.

719 *Piltz*, Soziale Netzwerke, S. 95 f.; *Ders./Trinkl*, in: Hoeren/Bensinger, Kap. 13, Rn. 138 ff.; *Plath*, in: Plath, § 1 BDSG, Rn. 33; *von Lewinsky*, in: Auernhammer, § 1 BDSG, Rn. 18; *Hornung/Hofmann*, JZ 2013, 163 (167 f.); Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 12, allerdings unter der Einschränkung, dass eine Nutzung der Daten durch den Anbieter ausgeschlossen sein muss; vgl. auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 76, 118.

720 *Piltz*, Soziale Netzwerke, S. 95; vgl. auch *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 135.

721 *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 135; vgl. auch *Gola/Lepperhoff*, ZD 2016, 9 (10); *Hornung/Hofmann*, JZ 2013, 163 (167 f.); *Plath*, in: Plath, § 1 BDSG, Rn. 33.

722 So auch *Dammann*, in: Simitis, BDSG, § 1 Rn. 151; vgl. auch *Buchholtz*, AöR 2015, 121 (147).

Raum der Straße mitüberwacht, nicht unter das Haushaltsprivileg fällt, da mit der Tätigkeit die rein private Sphäre objektiv verlassen wird.[723] Während freilich die Überwachung einer Straße nicht unmittelbar mit der Aktivität in sozialen Netzwerken vergleichbar ist, lässt sich doch die Aussage des EuGH übertragen, dass der Umfang der Anwendbarkeit des Haushaltsprivilegs sich nicht ausschließlich aus der individuell vorgenommenen privaten Zwecksetzung ergeben kann.

Die klassische Abgrenzung nach einer privaten oder einer beruflichen Zwecksetzung erweist sich zudem als zu grob für die Bedingungen und Risiken der Datenverarbeitung in sozialen Netzwerken. Auch wenn Inhaltsdaten nur innerhalb des sozialen Netzwerks oder sogar nur innerhalb eines „Freundes- und Bekanntenkreises" in diesem sozialen Netzwerk veröffentlicht werden, liegt typischerweise keine Konstellation vor, die als privat anzusehen wäre[724] und somit von dem Haushaltsprivileg erfasst sein sollte. Einerseits besteht eine ganz andere Risikolage – dazu sogleich –, andererseits ist auch nicht auszuschließen, dass die Daten von dem Anbieter des sozialen Netzwerks zu eigenen Zwecken genutzt werden und damit den privaten Kreis verlassen.[725] Anstatt nur nach der objektivierten Zwecksetzung zwischen den Sphären abzugrenzen, muss in Betracht gezogen werden, welcher Adressatenkreis potentiell von einer Datenübermittlung betroffen ist.[726] Dies soll im Folgenden durch eine grundrechtskonforme Auslegung des Haushaltsprivilegs gezeigt werden.

---

723 EuGH, *Frantisek Rynes*, Rs. C-212/13, Rn. 33 = EuZW 2015, 234 (236).

724 Ausdrücklich von „Veröffentlichung" spricht in diesem Zusammenhang *Redeker*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 12, Rn. 434; *Jandt/Roßnagel*, ZD 2011, 160 (162); vgl. auch *Buchholtz*, AöR 2015, 121 (148); a.A. *Gola/Lepperhoff*, ZD 2016, 9 (10); *Hornung/Hofmann*, JZ 2013, 163 (167 f.).

725 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 349. Die Abgrenzung der Konferenz der Datenschutzbeauftragten von Bund und Ländern, das Haushaltsprivileg für anwendbar zu erachten, wenn ein solcher Zugriff des Betreibers ausgeschlossen ist, erscheint daher arg künstlich und wenig praxisnah (Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 12). Gerade „kostenlose" soziale Netzwerke nutzen die Daten ihrer Nutzer, um Profite zu generieren. Dass sie nicht auf die gespeicherten Inhalte zurückgreifen, um Profile und Ähnliches zu erstellen, ist daher sehr unwahrscheinlich. Insbesondere im Falle von Facebook ist es zudem für die Nutzer faktisch unmöglich, ihre Inhalte dem Zugriff von Facebook zu entziehen, vgl. auch ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 18 f.

726 Vgl. auch *Dammann*, in: Simitis, BDSG, § 1 Rn. 151; EuGH, *Lindqvist*, Rs. C-101/01, Rn. 47 = EuR 2004, 291 (299); *Gola/Lepperhoff*, ZD 2016, 9 (10); *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 135; *Klar*, DÖV 2013, 103 (109); *Jandt/Roßnagel*, ZD 2011, 160 (162). Insofern wäre es aus Gründen der Rechtsklarheit sehr zu begrüßen gewesen, hätte sich die vom europäischen Parlament erarbeitete Fassung des Art. 2 Abs. 2 lit. d) DS-GVO-E a.F. durchgesetzt, welche ausdrücklich auf den zu erwartenden Verbreitungsgrad der Daten abstellte.

iii) Nutzung von sozialen Netzwerken als strukturelle Gefährderung der informationellen Selbstbestimmung Dritter

Wenn Nutzer personenbezogene Daten anderer Personen in einem sozialen Netzwerk posten, gefährden sie die informationelle Selbstbestimmung dieser Personen. Das Haushaltsprivileg übernimmt zwar eine wichtige Funktion dabei, die freie Kommunikation und private Selbstverwirklichung zu ermöglichen; es muss aber in einen angemessenen Ausgleich zu jener strukturellen Gefährdung der informationellen Selbstbestimmung gebracht werden.

Das Datenschutzrecht bietet keinen umfassenden Persönlichkeitsschutz Betroffener gegenüber anderen Privaten und garantiert auch kein absolutes Herrschaftsrecht über eigene Daten im persönlichen Verhältnis zu anderen. Das Grundrecht auf informationelle Selbstbestimmung kann nicht so weit verstanden werden, dass es ein implizites Recht beinhaltet, über das Gelingen der eigenen Selbstdarstellung gegenüber anderen zu verfügen, indem eigene Daten ausschließlich mit einer Einwilligung genutzt werden dürfen.[727] Es weist vielmehr dort Grenzen auf, wo Informationen überhaupt erst im sozialen Umgang mit anderen entstehen können und daher notwendig der Entscheidungsbefugnis des Einzelnen entzogen sind[728] oder das Funktionieren gesellschaftlicher Prozesse von einem freien Informationsfluss abhängig ist.[729] Das Recht auf informationelle Selbstbestimmung stellt sich somit weniger als materielles Verfügungsrecht über Daten und Informationen denn vielmehr als ein instrumentelles, prozedurales Sicherungsrecht dar, das die Rahmenbedingungen einer selbstbestimmten Persönlichkeitsentwicklung sicherstellen soll. Es schützt die Freiheit des Einzelnen, sich als Person finden zu können und sich hiernach zu verhalten, ohne massiv durch von ihm nicht beeinflussbare Fremdbilder und vorgefertigte Erwartungen anderer eingeschränkt zu sein.[730] Er soll sich darauf einstellen können, was andere von ihm wissen und erwarten können und dadurch informiert über seine Selbstdarstellung entscheiden bzw. „autonomiesichernde

---

727 *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 571 f.; *Hoffmann-Riem*, AöR 1998, 513 (523); *Taeger/Schmidt*, in: Taeger/Gabel, Einf BDSG, Rn. 33 m.w.N.; *Simitis*, in: Simitis, BDSG, § 1 Rn. 86; vgl. auch *Masing*, NJW 2012, 2603 (2307 f.); *Trute*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 2.5, Rn. 21 ff.

728 Zum Begriff der Information bereits oben unter B.II.1., zur informationellen Selbstbestimmug noch ausführlicher unten unter D.III.4.a); vgl. auch *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 571 f., mit zahlreichen Nachweisen dort in Fn. 37.

729 *Eifert*, Zweckvereinbarkeit, in: Gropp u.a. (Hrsg.), S. 145 m.w.N.; vgl. auch *Taeger/Schmidt*, in: Taeger/Gabel, Einf BDSG, Rn. 34.

730 *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 569 ff.; *Hoffmann-Riem*, AöR 1998, 513 (523 f.); *v. Lewinsky*, Matrix des Datenschutzes, S. 45; BVerfG 65, 1 (42 f.) – Volkszählungsurteil.

Selbstvergewisserungsprozesse“[731] durchlaufen können. Ein Wissensdefizit darüber, wie andere aufgrund einer Handlung über einen selbst denken und in welchem Kontext diese Handlung von wem beurteilt werden könnte, kann sehr abschreckend wirken und daher eine reale Freiheitseinschränkung bedeuten.[732] Der Schutzbereich der informationellen Selbstbestimmung ist damit beschränkt und verlangt mitnichten einen absoluten Schutz sämtlicher personenbezogener Daten.

In diesem Sinne ist aus grundrechtlicher Perspektive nichts dagegen einzuwenden, wenn der Gesetzgeber mit dem Haushaltsprivileg einen Bereich privater Lebensführung vom Anwendungsbereich des Datenschutzrechts ausnimmt und damit die Herrschaftsmöglichkeit des Betroffenen über konkrete Daten in materieller Hinsicht einschränkt.[733] Diese Einschränkung darf aber nicht so weit gehen, dass die prozedurale Dimension der informationellen Selbstbestimmung unverhältnismäßig beeinträchtigt, im Extremfall gar gänzlich negiert wird. Eine Datenverarbeitung, die ausschließlich innerhalb des persönlichen und familiären Kreises bzw. des engen Bekanntenkreises des Datenverarbeiters erfolgt, ist regelmäßig nicht geeignet, eine strukturelle Bedrohung für das instrumentell und prozedural verstandene Recht auf informationelle Selbstbestimmung eines Dritten darzustellen. Eine substantielle Einschränkung von innerer und äußerer Entfaltungsfreiheit des Betroffenen ist nicht zu erwarten, wenn die Nutzung der Daten auf einen so kleinen Kreis beschränkt bleibt.

Ebendiese Gefährdungslage stellt sich bei der privaten Datenverarbeitung in sozialen Netzwerken gänzlich anders dar. Zum einen sind die Daten stets auch dem Anbieter des sozialen Netzwerks zugänglich, nicht nur den anderen Nutzern.[734] Zum anderen weist der Umgang mit ihnen die strukturellen Besonderheiten des digitalen Datenumgangs in Netzwerken auf, insbesondere eine lange Speicherdauer, eine einfache Verknüpfbarkeit durch Suchfunktionen und eine Replizierbarkeit, indem die Daten kopiert und weiterverbreitet werden können, ohne dass diese Kopie zwingend als solche zu erkennen ist. Die Daten können hierdurch verhältnismäßig leicht einem großen Publikum zugänglich gemacht werden und über den ursprünglich intendierten Empfängerkreis weit hinausgehen.[735] Ein durchschnittlicher

731 *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 571.

732 *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 569; *Hoffmann-Riem*, AöR 1998, 513 (523 f.); BVerfG 65, 1 (42 f.) – Volkszählungsurteil.

733 Vgl. auch *v. Lewinsky*, Matrix des Datenschutzes, S. 10.

734 *Spiecker gen. Döhmann*, K&R 2012, 717 (722); *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 349; dies übersieht *Dammann*, in: Simitis, BDSG, § 1 Rn. 151.

735 Ausführlich hierzu: *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 44 ff.; vgl. auch *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 135; *Spiecker gen. Döhmann*, K&R 2012, 717 (722).

Facebooknutzer hat zahlreiche, im Zweifel mehrere hundert „Freunde", die auf seine Einträge in seinem Profil, insbesondere auf der „Pinnwand", Zugriff haben.[736] Diese sind untereinander im Zweifel nur dadurch verbunden, „Freunde" eines bestimmten Nutzers zu sein. Zwar filtert Facebook die Beiträge mit einem Algorithmus, so dass längst nicht jedem Nutzer alle Beiträge angezeigt werden[737]. Der postende Nutzer hat aber keinen direkten Einfluss, wem dieser Freunde infolge des Algorithmus' seine geposteten Beiträge angezeigt werden. Er muss also davon ausgehen, dass sie zumindest theoretisch doch für jeden dieser Freunde sichtbar sind. Zusätzlich können die Freunde jedenfalls „manuell" jederzeit auf sein Profil zugreifen und auf der Pinnwand geteilte Beiträge lesen und ihrerseits weiterverbreiten. Selbst wenn die Privatsphäre-Einstellungen so gewählt wurden, dass nur eigene Freunde die Einträge im Profil und auf der Pinnwand sehen können, kann daher durch die Option des „Teilens" oder Copy-Paste der ursprünglichen Nachricht in weiteren Profilen mit wenigen Mausklicks eine erhebliche Weiterverbreitung stattfinden, die der Kontrolle des die Inhalte ursprünglich übermittelnden Nutzers entzogen ist.[738] Im Extremfall kann es daher zu einer Verbreitung der Information bis zu jedem einzelnen Nutzer des sozialen Netzwerks kommen[739] oder sogar noch darüber hinaus, wenn einer der weiterverbreitenden Nutzer sein Profil der Öffentlichkeit des gesamten Internets zugänglich gemacht hat oder eine Indexierung durch Suchmaschinen nicht ausgeschlossen hat.[740]

Das Verarbeiten fremder Daten in sozialen Netzwerken durch andere Nutzer ist somit geeignet, Fremdbilder über den Betroffenen mit einer ganz erheblichen Reichweite zu verbreiten und damit die innere und äußere Entfaltungsfreiheit des Betroffenen massiv einzuschränken. Es ist strukturell keinesfalls vergleichbar mit einem privaten Adressbuch oder digitalen Fotoalbum

---

736 In den USA lag die durchschnittliche Anzahl der Freunde über alle Altersgruppen hinweg im Jahr 2014 bei 350, in jüngeren Altersgruppen zum Teil deutlich höher http://de.statista.com/statistik/daten/studie/325772/umfrage/durchschnittliche-anzahl-von-facebook-freunden-in-den-usa-nach-altersgruppe/.

737 Bis 2012 als „Edgerank" bezeichnet, vgl. *Pariser*, Filter Bubble, S. 37 f.; Während Facebook offiziell diesen Namen nicht mehr für den Algorithmus verwendet, soll er hier in Ermangelung eines besseren offiziellen Begriffs – wo nötig – verwendet werden.

738 Man kann sich freilich fragen, wie oft und entsprechend wie wahrscheinlich es zu einer derartigen Weiterverbreitung kommt. Soziale Netzwerke leben zu einem nicht unerheblichen Teil von einer Kultur des Teilens und Weiterverbreitens von Inhalten. Entsprechend ist es jedenfalls nicht unüblich, einen Beitrag eines Bekannten zu teilen oder weiterzuverbreiten, wenn dieser als interessant empfunden wird, so dass es sich um ein durchaus realistisches Szenario handelt.

739 Im Falle von Facebook eine Öffentlichkeit von 1,6 Mrd. Menschen, http://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/.

740 Vgl. hierzu auch *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S.44 ff.; *Gola/Lepperhoff*, ZD 2016, 9 (11); *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 349; *Dies./Ders.*, ZD 2011, 160 (162).

für den rein familiären Gebrauch, wie es nach der hier aufgezeigten grundrechtskonformen Auslegung und dem Wortlaut des Erwägungsgrundes 18 DS-GVO dem Haushaltsprivileg zugrunde liegt. Eine derartige Datenverarbeitung unter eine ausschließlich persönliche oder familiäre Tätigkeit zu subsumieren, wäre daher verfehlt.[741]

Vertreter der Ansicht, die Nutzern in sozialen Netzwerken für private Datenverarbeitung das Haushaltsprivileg zusprechen, bringen hiergegen vor, dass Abgrenzungsschwierigkeiten drohten, ab wie vielen „Freunden" von einer Versagung des Privilegs auszugehen wäre und somit eine willkürliche Entscheidung drohe.[742] Das Risiko weiterer Datenverarbeitungen und -weitergaben durch Dritte, insbesondere auch den Anbieter des sozialen Netzwerks, soll zudem unbeachtlich sein, da es auf eine „mittelbare Verantwortlichkeit der privat agierenden Nutzer" hinausliefe, „die dem Datenschutzrecht jedoch fremd ist".[743]

Beide Einwände gehen fehl. Angesichts der aufgezeigten Grundrechtsrelevanz kann es bereits nicht überzeugen, die Ausnahmevorschrift allein deshalb standardmäßig anzuwenden, weil es auch Einzelfälle geben könnte, in denen ein Nutzer tatsächlich nur so wenige Freunde in einem sozialen Netzwerk hat, dass es sich von seinem persönlichen und familiären Kreis nicht substantiell unterscheidet. Dies gilt umso mehr, als die Bundesrepublik Deutschland völkerrechtlich durch die Datenschutzkonvention des Europarates[744] gebunden ist, welche in ihrem Art. 9 Abs. 2 eine datenschutzrechtliche Privilegierung nur für Fälle vorsieht, in denen dies „in einer demokratischen Gesellschaft […] zum Schutz des Betroffenen oder zum Schutz der Rechte und Freiheiten Dritter" notwendig ist.[745] Die Ausnahmevorschrift ist daher grundsätzlich restriktiv anzuwenden und auf Fälle zu begrenzen, wo dies zur Wahrung von Grundrechten des Verantwortlichen erforderlich und angemessen ist.[746]

Weiterhin ergibt sich die strukturelle Gefährdung der informationellen Selbstbestimmung des Betroffenen nicht so sehr aus der konkreten Zahl der „Freunde" des Nutzers, sondern aus der

---

741 So im Ergebnis auch bereits *Maisch*, Informationelle Selbstbestimmung, S. 203 f., der aber Zweifel äußert, ob private Nutzer in dieser Rolle tatsächlich dem Datenschutzrecht unterworfen werden sollten. A.A., allerdings ohne nähere Begründung, *Dix*, in: Simitis, BDSG, § 35 Rn. 8; *Gola/Lepperhoff*, ZD 2016, 9 (10), welche zwar das Risiko der möglichen Weiterverbreitung durch die Empfänger erkennen und kritisieren, aber dennoch eine Anwendbarkeit des Haushaltsprivilegs bejahen, soweit der Kreis der Empfänger auf einen engen Familien- und Freundeskreis beschränkt ist; *Piltz*, Soziale Netzwerke, S. 96.

742 *Piltz*, Soziale Netzwerke, S. 95.

743 *Piltz*, Soziale Netzwerke, S. 96.

744 Konvention 108, BGBl. II 1985, S. 538.

745 *Dammann*, in: Simitis, BDSG § 1 Rn. 148; *Schmidt*, in: Taeger/Gabel, § 1 BDSG, Rn. 30.

746 *Schmidt*, in: Taeger/Gabel, § 1 BDSG, Rn. 30; *Dammann*, in: Simitis, BDSG § 1 Rn. 148; *Piltz*, Soziale Netzwerke, S. 93; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 349; *Dies./Ders.*, ZD 2011, 160 (162).

einfachen Möglichkeit der Weiterverbreitung, die durch die technische Infrastruktur und netzwerktypische Kultur des „Teilens“ gegeben ist und die in dieser Effizienz und potentiellen Reichweitenwirkung keine analoge Entsprechung in einem privaten und familiären Kreis findet. Es erübrigt sich somit, eine feste Grenze zu ziehen, ab welcher Zahl von „Freunden“ in einem sozialen Netzwerk die Anwendbarkeit des Haushaltsprivilegs zu verneinen wäre, da selbst bei nur ein oder zwei Freunden[747] die einfache technische Möglichkeit der Weiterverbreitung bestünde und somit eine strukturelle Gefährdungslage für die informationelle Selbstbestimmung geschaffen wird. Auch die spätere Verwendung der Daten durch den Anbieter des sozialen Netzwerks kann nicht durch den Nutzer kontrolliert werden. Selbst wenn der Nutzer die Sichtbarkeit der Daten auf eine kleine Handvoll enger Bekannter beschränkt, verlassen sie daher die private Sphäre des Nutzers, so dass das Haushaltsprivileg nicht anzuwenden ist.[748]

Auch der Vorwurf, dass hierdurch eine „mittelbare Verantwortlichkeit der privat agierenden Nutzer“ begründet würde[749], trifft nicht zu. Die Frage der Anwendbarkeit des Haushaltsprivilegs betrifft nicht die Zuschreibung von Verantwortlichkeit, sondern die Auslegung des Tatbestandsmerkmals der „ausschließlich familiären und persönlichen Tätigkeiten“. Ob eine Verantwortlichkeit und überhaupt eine relevante Datenverarbeitung vorliegen, ist erst im Anschluss durch eine Auslegung der verschiedenen Tatbestände der Datenschutzgesetze zu beurteilen. Dies kann im Einzelfall schwierig zu beurteilen sein und sollte daher nicht gänzlich dem Anwendungsbereich des Datenschutzrechts entzogen werden.[750] Der richtige Ort für diese Abwägung ist vielmehr im Rahmen der Verhältnismäßigkeitsprüfung, die durch die gebotenen Interessenabwägungen nach §§ 28, 29 BDSG bzw. zukünftig Art. 6 Abs. 1 lit. f) DS-GVO vorzunehmen ist.[751]

Die neuen strukturellen Gefährdungslagen, die soziale Netzwerke für die informationelle Selbstbestimmung von Nutzern schaffen, zwingen mithin dazu, in einer grundrechtskonformen Auslegung des Begriffs der persönlichen und familiären Tätigkeiten den potentiellen Adressatenkreis einer Handlung mit in den Blick zu nehmen. Die Privilegierung kann nur dann Anwendung finden, wenn der Nutzer berechtigterweise davon ausgehen kann, dass seine

747 Ein praktisch wohl extrem seltener Fall, vgl. http://de.statista.com/statistik/daten/studie/325772/umfrage/durchschnittliche-anzahl-von-facebook-freunden-in-den-usa-nach-altersgruppe/.

748 So auch schon *Jandt/Roßnagel*, ZD 2011, 160 (162); *Dies./Ders.*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 349; a.A. *Dix*, in: Simitis, BDSG, § 35 Rn. 8.

749 *Piltz*, Soziale Netzwerke, S. 96.

750 Vgl. *Buchholtz*, AöR 2015, 121 (136).

751 Hierzu noch ausführlich unten unter D.I.3.b)bb)iii).

Datenverarbeitung nur in einem mit seinem familiären oder persönlichen Umfeld vergleichbaren Kreis Wirkung entfaltet.[752] Dies ist bei der Übermittlung von personenbezogenen Daten in soziale Netzwerke nicht der Fall.

iv) Zwischenergebnis

Eine Anwendbarkeit des Haushaltsprivilegs auf die Verarbeitung personenbezogener Daten Dritter durch Nutzer in sozialen Netzwerken ist daher sowohl nach bisheriger als auch nach zukünftiger Rechtslage abzulehnen. Die Nennung der Nutzung sozialer Netzwerke in Erwägungsgrund 18 DS-GVO widerspricht der Gesamtkonzeption des europäischen Datenschutzrechts und verkennt die verbundenen Risiken und strukturellen Besonderheiten der Datenverarbeitung in sozialen Netzwerken. Sie ist daher teleologisch auf Offline-Kontexte zu reduzieren. In einem Online-Kontext kann sie allenfalls in praktisch kaum denkbaren Fällen herangezogen werden, in denen Nutzer ausschließlich persönliche Bekanntschaften in ihrem sozialen Netzwerk haben, welche die Daten nicht unkontrolliert weiterverbreiten können und ein Zugriff des Anbieters des sozialen Netzwerks auf die Daten ausgeschlossen ist.

bb) Datenschutzrechtliche Verantwortlichkeit der Nutzer

Eine datenschutzrechtliche Verantwortlichkeit der Nutzer in sozialen Netzwerken ist nach hier vertretener Auffassung nicht grundsätzlich gemäß § 1 Abs. 2 Nr. 3 BDSG bzw. Art. 2 Abs. 2 lit. c) DS-GVO ausgeschlossen. Dennoch ist problematisch, inwieweit sie als „Verantwortliche“ im Sinne des Datenschutzrechts angesehen werden können. Schwierigkeiten rühren insbesondere daher, dass die Nutzer zwar alleine die Entscheidung über das „Ob“ der Datenverarbeitung treffen, indem sie darüber bestimmen können, welche Daten über Dritte sie Preis geben, sie aber zugleich keinerlei Entscheidungsbefugnis hinsichtlich des „Wie“ der Datenverarbeitung haben, da dies allein durch den Anbieter des sozialen Netzwerks geregelt wird.

Wie oben bereits dargelegt, plädieren daher *Roßnagel* und *Jandt* für eine „kollektive Verantwortung“[753] von Nutzern und Anbietern, ohne allerdings genau darzulegen, welche konkreten Schritte der Datenverarbeitung die Nutzer vornehmen. Die Verantwortungsbereiche sollen strikt voneinander getrennt sein und nebeneinander bestehen. Soweit dies eine Entlastung

---

752 *Gola/Lepperhoff*, ZD 2016, 9 (10 f.); ebenfalls bereits in diese Richtung *Klar*, DÖV 2013, 103 (109); vgl. auch Art. 2 Abs. 2 lit.d) DS-GVO-E in der Fassung des *LIBE*-Entwurfs des europäischen Parlaments.

753 *Jandt/Roßnagel*, ZD 2011, 160 (161); ihnen folgend *Kroschwald*. ZD 2014, 388 (389).

des Anbieters bedeutet, die damit begründet wird, dass dieser nicht über das konkrete „Ob" einer Datenverarbeitung bestimmen kann, ist dem nicht zu folgen.[754] An dieser Stelle interessiert nun allerdings, welche Datenverarbeitung Nutzer in sozialen Netzwerken vornehmen, welche datenschutzrechtlichen Pflichten – in Abgrenzung zu möglicherweise parallel bestehenden, hier nicht näher behandelten zivilrechtlichen Pflichten[755] – sich hieraus ergeben können[756] und nach welchen Erlaubnistatbeständen die Datenverarbeitung gerechtfertigt sein kann.

i) Datenübermittlung und hieraus resultierende datenschutzrechtliche Pflichten

Indem Nutzer personenbezogene Daten in das „Formular" der Anbieter sozialer Netzwerke eingeben, stellen sie diese Daten dem Anbieter sowie weiteren Nutzern zur Verfügung. In der differenzierten Terminologie des nationalen Datenschutzrechts kann es sich hierbei nur um eine Speicherung von Daten i.S.v. § 3 Abs. 4 Nr. 1 BDSG oder eine Übermittlung von Daten i.S.v. § 3 Abs. 4 Nr. 3 BDSG handeln. Eine Erhebung von Daten i.S.v. § 3 Abs. 3 BDSG scheidet dagegen aus, da der Nutzer die Daten über den Betroffenen durch die Veröffentlichung im sozialen Netzwerk nicht „beschafft".[757] Er verfügt vielmehr bereits über diese Daten und teilt diese lediglich weiteren Personen mit. Die Übermittlung eigener Daten ist dabei nicht von datenschutzrechtlicher Relevanz, da die Regelungen des BDSG grundsätzlich nicht anzuwenden sind, wenn jemand Daten zu seiner eigenen Person verarbeitet.[758] Auch hier geht es damit um nutzergenerierte Inhaltsdaten über Dritte.

Die Begriffe des Speicherns und Übermittelns sind medien- und technikneutral zu verstehen und damit weit auszulegen. Von einer Speicherung kann daher bereits bei jeder Erfassung von Daten in einer verkörperten Form durch eine Bedienung eines Datenerfassungsgeräts ausgegangen werden. Auf die genaue Art der Fixierung, also den Code, die Sprache oder das Signal, kommt es dagegen nicht an.[759] Eine Übermittlung stellt ebenso technikneutral

754 Hierzu bereits ausführlich oben unter D.I.3.a).

755 Ausführlich zur zivilrechtlichen Verantwortlichkeit *Hollenders*, Mittelbare Verantwortlichkeit, S. 46 ff.; *Lauber-Rönsberg*, MMR 2014, 10 (11 ff.); *Piltz*, Soziale Netzwerke, S. 192 ff.

756 *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 118 weist zutreffend darauf hin, dass es bei der Umsetzung der datenschutzrechtlichen Pflichten teilweise zu erheblichen Schwierigkeiten kommen kann, da diese häufig nicht auf private Nutzer zugeschnitten sind.

757 Zukünftig formal alles eine nicht detailliert legaldefinierte „Datenverarbeitung" gemäß Art. 4 Nr. 2 DS-GVO. Zur dogmatischeren Handhabung wird daher auch hier auf die differenzierteren Begriffe des BDSG zurückgegriffen.

758 *Dammann*, in: Simitis, BDSG, § 3 Rn. 226.

759 *Dammann*, in: Simitis, BDSG, § 3 Rn. 115; *Buchner*, in: Taeger/Gabel, § 3 BDSG, Rn. 28; *Plath/Schreiber*, in: Plath, § 3 BDSG, Rn. 35.

interpretiert jegliche Weitergabe dar, „durch die die in den Daten enthaltene Information in den Bereich des Adressaten gelangt“.[760]

Selbst in dieser weiten Fassung ist indes zweifelhaft, inwieweit diese Tatbestände auf die Nutzer sozialer Netzwerke zutreffen. Die Nutzer sind ohne Frage die Veranlasser der konkreten Erfassung der Daten von Betroffenen, indem sie bestimmen, welche Daten preisgegeben werden und das Eingabegerät bedienen. Allerdings haben sie keinerlei Einfluss auf die Speicherungsmechanismen, die im Hintergrund des sozialen Netzwerks geschehen. Sie können nicht beeinflussen, wie, wo und in welcher Form die Daten gespeichert werden. Faktisch bitten sie nur den Anbieter des sozialen Netzwerks, die von ihnen bereit gestellten Daten für sie zu speichern und für einen späteren Abruf bereit zu halten. Für dieses Auseinanderfallen von Veranlasser und Handelndem sehen das BDSG und die DS-GVO die Figur des Auftragsdatenverarbeiters vor. Eine solche Vereinbarung zwischen dem Anbieter und dem Nutzer eines sozialen Netzwerks anzunehmen, wäre indes lebensfremd und eine bloße Fiktion, da der Nutzer dem Anbieter gegenüber mitnichten weisungsbefugt ist. Vielmehr besteht ein klares Machtgefälle zulasten des Nutzers, welcher sich sowohl dem Code als auch den AGB des Anbieters zu unterwerfen hat und keine Möglichkeit der individuellen Aushandlung von Bedingungen und Konditionen der Auftragsdatenverarbeitung hat. Diese Möglichkeit wird in § 11 Abs. 2 und 3 BDSG bzw. Art. 26 Abs. 2 DS-GVO aber vorausgesetzt. Der Anbieter eines sozialen Netzwerks ist somit nicht als Auftragsdatenverarbeiter anzusehen, soweit die Nutzer Inhaltsdaten einstellen und von ihm speichern lassen.[761] Entsprechend müssen die Nutzer sich die Speicherung mangels einer Stellung als Auftraggeber auch nicht zurechnen lassen und nehmen mithin keine „Speicherung“ der Daten vor.

Die Nutzer übermitteln allerdings Daten, wenn sie personenbezogene Daten über Dritte in das soziale Netzwerk einstellen. Durch die Eingabe kommt es zur (Zwischen-)Speicherung auf den Servern des Anbieters des sozialen Netzwerks. Sie gelangen damit in dessen Einflussbereich. Dass der Anbieter für viele Nutzer vielleicht nicht der primäre Adressat der Datenübermittlung ist, sondern andere Nutzer, kann an dieser Stelle nicht entscheidend sein. Das Übermitteln von Daten stellt einen objektiven Vorgang dar, welcher nicht nach dem subjektiven technischen Verständnis des Übermittelnden zu beurteilen ist. Soweit man überhaupt eine subjektive Komponente anerkennen will, muss es ausreichen, wenn dem Übermittler bewusst ist, dass er

---

760 *Dammann*, in: Simitis, BDSG, § 3 Rn. 146; vgl. auch *Buchner*, in: Taeger/Gabel, § 3 BDSG, Rn. 35; *Plath/Schreiber*, in: Plath, § 3 BDSG, Rn. 42.

761 Vgl. auch *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 351; *Dies./Ders.*, ZD 2011, 160 (163 f.);

Daten in ein IT-System speichern lässt, in dem diese abrufbar sind. Der EuGH hat hierzu bereits 2003 in der *Lindqvist*-Entscheidung festgestellt, dass der „Vorgang, der darin besteht, personenbezogene Daten auf eine Internetseite zu stellen" als Datenverarbeitung anzusehen ist.[762]

Man könnte zwar am Vorliegen einer „Übermittlung" zweifeln, da § 3 Abs. 4 Nr. 3 BDSG verlangt, dass es sich um ein Bekanntgeben „gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten" handeln muss. Man könnte insofern annehmen, dies sei nicht der Fall, wenn Nutzer personenbezogene Daten Dritter in die Eingabemasken sozialer Netzwerke einstellen, da diese vorher nicht als digitale Informationen vorlagen, sie mithin nicht „gespeichert" waren. Dieser Einwand beruht indes auf einem zu engen und sehr technikgebundenen Verständnis der Voraussetzung der gespeicherten Daten. Versteht man den Begriff des Übermittelns und der Speicherung technikneutral, so kann es auch für die übermittelten Daten nicht darauf ankommen, ob sie zuvor als digital gespeicherte Informationen auf einem Medium vorlagen und wie im Einzelnen der Vorgang der Informationsvermittlung erfolgt ist.[763] Vielmehr handelt es sich auch bei personenbezogenen Daten, die beispielsweise biochemisch im Gehirn eines übermittelnden Nutzers oder analog auf Papier gesichert waren, um gespeicherte Daten im Sinne von § 3 Abs. 4 Nr. 3 BDSG. Das erstmalige digitale Speichern kann folglich mit einer Übermittlung zeitlich zusammenfallen. Im Falle der Datenweitergabe an den Anbieter und andere Nutzer des sozialen Netzwerks liegt eine Bekanntgabe vor, bei welcher der Personenkreis vergrößert wird, dem die in den Daten enthaltenen Informationen zugänglich sind.[764] Es handelt sich mithin um eine Übermittlung personenbezogener Daten gemäß § 3 Abs. 4 Nr. 3 BDSG.[765]

Soweit Nutzer personenbezogene Daten über Dritte an das soziale Netzwerk übermitteln, sind sie also hierfür datenschutzrechtlich Verantwortliche. Ihnen kommen daher insoweit auch datenschutzrechtliche Pflichten zu, insbesondere die Benachrichtigungspflicht nach

---

762 EuGH, *Lindqvist*, Rs. C-101/01, Rn. 25 = EuR 2004, 291 (297); jüngst bestätigt in EuGH, *Weltimmo*, Rs. C-230/14, Rn. 37 = ZD 2015, 580 (582); zustimmend auch *Piltz*, Soziale Netzwerke, S. 92 f.; *Buchner*, in: Taeger/Gabel, § 3 BDSG, Rn. 36; *Weichert*, in: DKWW, § 3 BDSG, Rn. 37; kritisch *Klar*, DÖV 2013, 103 (108 f.)..

763 *Dammann*: in: Simitis, BDSG, § 3 Rn. 145.

764 *Dammann*: in: Simitis, BDSG, § 3 Rn. 145; vgl. auch *Buchner*, in: Taeger/Gabel, § 3 BDSG, Rn. 35.

765 So auch *Piltz*, Soziale Netzwerke, S. 93; wohl ebenfalls zustimmend, auch wenn die Verantwortlichkeit nur untechnisch an einer Veröffentlichung, bzw. einem Einstellen der Daten festgemacht wird: *Jandt/Roßnagel*, ZD 2011, 160 (164 f.); die Verantwortlichkeit bejahen auch *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (124 f.); *Buchner*, in: Taeger/Gabel, § 3 BDSG Rn. 36.

§ 33 BDSG bzw. 13 und 14 DS-GVO[766], sowie ggf. eine Berichtigungs- und Löschungsverpflichtung gemäß § 35 BDSG bzw. Art. 16 und 17 DS-GVO.[767]

ii) Datenübermittlung durch Zugriffsmöglichkeiten integrierter Apps

Einige Apps, die insbesondere in die Nutzung von Facebook integriert werden können, verlangen darüber hinaus von Nutzern, ihnen einen Zugriff auf für diese sichtbare Daten ihrer Facebook-Kontakte zu geben. Wenn ein Nutzer hierin einwilligt, werden diese Daten seiner Kontakte an den Betreiber oder Entwickler dieser App weitergegeben.[768] Für die betroffenen Dritten stellt sich auch diese Weitergabe als eine Übermittlung der Daten i.S.v. § 3 Abs. 4 Nr. 3 BDSG und damit auch Art. 4 Nr. 2 DS-GVO dar, da der Kreis derjenigen, die einen Zugriff auf die Daten haben, vergrößert wird. Diese Erweiterung ist insbesondere dann problematisch, wenn es sich um Daten handelt, die die betroffenen Dritten in ihren Privatsphäre Einstellungen nur für ihre Kontakte sichtbar gemacht haben und trotzdem über die Nutzung der App durch einen der Kontakte auch für den Betreiber der App sichtbar werden können.[769] Diese Übermittlung von Daten durch andere Nutzer kann von Betroffenen nur dann vermieden werden, wenn sie in ihrem eigenen Profil die Anwendungsplattform für Anwendungen von Drittanbietern vollständig deaktivieren und damit selbst auf die Nutzung von erweiterten Funktionen verzichten.[770] Diese „Alles-Oder-Nichts" Einstellung wurde bereits 2011 und 2012 in den Datenschutzaudits des irischen Datenschutzbeauftragten zu Recht kritisiert. Kritisiert wurde zudem, dass die Funktion für die Betroffenen nicht intuitiv auffindbar sei, da sie nicht in

---

766 Freilich gelten auch hier die bereits unter D.I.3.a)bb)iii) dargelegten Einschränkungen.

767 a.A. *Dix*, in: Simitis, BDSG, § 35 Rn. 8; Die datenschutzrechtlichen Pflichten sind hierbei freilich auf das begrenzt, was die Nutzer technisch leisten können, da das Recht keine unmöglichen Pflichten auferlegen darf. Entsprechend genügt insbesondere zur Erfüllung der Löschungsverpflichtung, die übermittelten Daten im eigenen Profil zu „löschen" und damit den Anbieter des sozialen Netzwerks über das Löschungsbegehren in Kenntnis zu setzen. Ob dieser die Löschung von seinen Servern tatsächlich vornimmt, kann von den Nutzern natürlich nicht beeinflusst werden und liegt entsprechend auch nicht in ihrem Pflichtenrahmen. Dennoch handelt es sich allenfalls um eine Teilunmöglichkeit, da bereits durch das „Löschen" durch den Nutzer die Daten nicht mehr für andere Nutzer einsehbar sind. Nur auf technischer Ebene muss die Löschung auch durch den Anbieter erfolgen, um sicherzustellen, dass die Daten nicht nur verborgen sind, sondern auch tatsächlich von den Servern entfernt werden. Dem primären Ziel eines Löschungsbegehrens, nämlich die Entfernung des ursprünglichen Datums aus der öffentlichen Wahrnehmbarkeit, kann ein Nutzer daher stets nachkommen. Vgl. zur möglichen Reduzierung der Pflichten trotz einer bestehenden datenschutzrechtlichen Verantwortlichkeit auch *Moos*, in: Taeger/Gabel, § 11 TMG, Rn. 32.

768 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 35; *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 90 f.

769 Prinzipiell gibt es bei Facebook für Betroffene in ihren erweiterten Privatsphäre Einstellungen die Möglichkeit zu einem Opt-Out aus Teilen dieser Datenübermittlung. Standardmäßig ist fast eine vollständige Weitergabe der eigenen Profildaten aktiviert – hiervon können viele, etwa ein Einblick auf die Pinnwandeinträge oder das Geburtsdatum, manuell abgewählt werden. Einer Weitergabe der „öffentlich einsehbaren" Daten wie dem Namen oder des Profilfotos kann aber nicht widersprochen werden.

770 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 35.

den Privatsphäre Einstellungen, sondern vielmehr den Anwendungs-Einstellungen verortet sei.[771] Diese Probleme bestehen bis heute fort.[772] Die Einstellungsoptionen erfüllen daher nicht die Anforderungen an eine rechtlich wirksame Einwilligung durch die Betroffenen.[773]

Sehr fraglich ist aber, ob es sich hierbei um eine den Nutzern zuzurechnende Übermittlung handelt, für die sie datenschutzrechtlich als verantwortliche Stelle einzustufen sind. Sie kontrollieren weder die Mittel noch die Zwecke, mit denen diese Daten erhoben werden, noch nehmen sie die Übermittlung eigenhändig vor. Darüber hinaus dürfte den wenigsten Nutzern bekannt sein, dass es überhaupt zu dieser Datenübermittlung durch ihre Nutzung der Anwendung des Drittanbieters kommt. Soweit hierauf überhaupt vor der Nutzung der Anwendung hingewiesen wird, erfolgt dies in einem langen Dokument mit weiteren datenschutzrechtlichen Bestimmungen, deren Bestimmtheit und Effektivität hinsichtlich der Aufklärung ohnehin zweifelhaft sind.[774] Ein möglicher Zugriff der Anwendung auf Daten, die von den Kontakten zur Verfügung gestellt wurden, stellt eine verhältnismäßig überraschende Regelung dar, an die viele Nutzer in diesem Moment eher nicht denken und daher im Zweifel auch nicht zur Kenntnis nehmen. Eine datenschutzrechtliche Verantwortlichkeit jenseits einer kausalen Verursachung der Datenübermittlung würde daher auf einer reinen Fiktion beruhen.

Nutzer sozialer Netzwerke sind daher nicht verantwortlich für eine Übermittlung von für sie sichtbarer Daten ihrer Kontakte, die automatisch erfolgt, wenn die Nutzer Anwendungen von Drittanbietern innerhalb des sozialen Netzwerks nutzen. Etwas anderes gilt nur dann, wenn eine klare und bestimmte Aufklärung über diese Datenübermittlung erteilt wird und für die Nutzer die Möglichkeit besteht, sich bewusst für oder gegen diese zu entscheiden, ohne dass hierbei eine „Alles-Oder-Nichts“ Entscheidung hinsichtlich der Nutzung der Anwendung getroffen werden muss.

iii) Erlaubnistatbestände

Soweit die Nutzer personenbezogene Daten über Dritte an den Anbieter des sozialen Netzwerks übermitteln, bedürfen sie hierfür einer gesetzlichen Erlaubnis oder einer Einwilligung des Betroffenen. Diese aus der unter D.I.3.b)aa) ausgiebig erörterten teleologische Reduktion des

---

771 *Irish Data Protection Commissioner*, Report of Re-Audit, 21.09.2012, S. 30 f.; *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 90 f.

772 Ein Opt-Out setzt immer noch voraus, sich mit Einstellungen zu befassen, die nicht alle unter dem Punkt „Privatsphäre“ vereint, sondern über verschiedene Menüs verteilt sind, vgl. u.a.: https://www.facebook.com/settings?tab=privacy; https://www.facebook.com/settings?tab=applications.

773 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 43; zur Einwilligung noch ausführlich unten unter D.III.2.

774 Vgl. unten unter D.III.2.b).

Haushaltsprivilegs resultierende Konsequenz ist nur vertretbar, wenn es Erlaubnistatbestände gibt, die einen hinreichenden Ausgleich von Äußerungsinteressen der datenverarbeitenden Nutzer und den Betroffeneninteressen schaffen.

Das BDSG sieht mit den §§ 28 ff. BDSG für nichtöffentliche Stellen allerdings nur Erlaubnistatbestände für geschäftsmäßige Datenverarbeitungen vor. Eine zu rein privaten Zwecken erfolgende Speicherung und Veröffentlichung von Daten Dritter in privaten Profilen sozialer Netzwerke als „geschäftsmäßig" zu bezeichnen ist widersinnig und überschreitet offensichtlich die Wortlautgrenze. Ab Geltung der DS-GVO wird allerdings der allgemeine Erlaubnistatbestand des Art. 6 Abs. 1 lit.f) DS-GVO die Interessenabwägung nicht mehr auf geschäftsmäßige Zwecke beschränken und sie damit auch unmittelbar für private Zwecke eröffnen. Die notwendige Abwägung kann sodann unproblematisch vorgenommen werden.

Auch nach der bisherigen Rechtslage ist allerdings ein Interessenausgleich möglich, indem die §§ 28 ff. BDSG analog auf eine Datenverarbeitung zu persönlichen Zwecken angewendet werden. Angesichts der bisher verbreiteten extensiven Auslegung des Haushaltsprivilegs verwundert es nicht, dass eine Anwendbarkeit der §§ 28 ff. BDSG auf private Datenverarbeitung in sozialen Netzwerke nur sehr sporadisch – wenn überhaupt – diskutiert wurde und in Kommentierungen ein klarer Fokus auf den unterschiedlichen geschäftsmäßigen Formen der Datenverarbeitung liegt.[775] Häufig finden sich allenfalls kurze Feststellungen, dass das berechtigte Interesse an der Datenverarbeitung zur Erfüllung eigener Geschäftszwecke nicht zwingend wirtschaftlicher Natur sein muss, sondern auch ein ideelles Interesse darstellen kann.[776]

Es ist dem technischen Fortschritt geschuldet, dass Privatleute heute überhaupt in der Lage sind, Datenverarbeitungen vorzunehmen, die datenschutzrechtliche Relevanz besitzen. Zuvor war es nicht erforderlich, Erlaubnistatbestände für private Datenverarbeitungen zu erlassen, da diese aufgrund des Haushaltsprivilegs nicht dem Anwendungsbereich und damit dem Verbot mit Erlaubnisvorbehalt des Datenschutzrechts unterfielen. Aus der historischen Perspektive ist die Begrenzung auf geschäftsmäßige Datenverarbeitung sehr verständlich, da es in der Zeit vor (effizienten) Suchmaschinen, Internetforen und sozialen Netzwerken – also noch vor weniger als zwanzig Jahren – wohl kaum vorstellbar war, dass rein private Nutzer überhaupt die Möglichkeit zu datenschutzrechtlich relevanter Datenverarbeitung bekommen würden. Es liegt

---

775 Vgl. z.B. *Simitis*, in: Simitis, BDSG, § 28 Rn. 22 ff., 52 ff., 98 ff.; *Plath*, in: Plath, § 28 BDSG, Rn. 29 ff., 55 ff.; anders, allerdings sehr knapp, *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 37.

776 *Simitis*, in: Simitis, BDSG, § 28 Rn. 104; vgl. auch *Plath*, in: Plath, § 29 BDSG, Rn. 87.

daher bis zur Anwendbarkeit der DS-GVO eine planwidrige Regelungslücke vor, die durch Auslegung zu schließen ist und eine Analogie zulässig macht.[777] Auch mit Anwendbarkeit der DS-GVO bleibt die im Folgenden aufgezeigte Analyse der betroffenen Grundrechte relevant, um die nach Art. 6 Abs. 1 lit. f) DS-GVO vorzunehmende Interessenabwägung dogmatisch zu strukturieren.

Gemäß § 28 Abs. 1 S. 1 Nr. 2 BDSG ist die Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen zulässig, sofern dies für die Erfüllung eigener Geschäftszwecke erforderlich ist. Diese Möglichkeit der Interessenabwägung sorgt somit für eine Verhältnismäßigkeit des Prinzips der Datensparsamkeit und des Verbots mit Erlaubnisvorbehalt, welche durch § 4 Abs. 1 BDSG statuiert werden. Mit der Möglichkeit privater Datenverarbeitung werden die berechtigten wirtschaftlichen Verarbeitungsinteressen ergänzt um kommunikative und persönlichkeitsbildende Interessen, die durch die Meinungsfreiheit gemäß Art. 5 Abs. 1 S. 1 Alt. 1 GG[778], aber auch das allgemeine Persönlichkeitsrechts gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützt sind.[779] Letzteres mag zunächst überraschen, wird das allgemeine Persönlichkeitsrecht doch in der Regel als Rechtfertigung für den Datenschutz und die Geheimhaltung von Daten angeführt. Hierbei ist aber zu beachten, dass das Persönlichkeitsrecht – und speziell das Recht auf informationelle Selbstbestimmung – nicht nur das Recht auf Geheimhaltung von Menschen schützt, sondern auch das Recht auf gezielte Preisgabe von Daten zur Selbstdarstellung.[780] Hiermit sind natürlich primär eigene Daten gemeint. Allerdings muss dabei berücksichtigt werden, dass Menschen sich sozial über ihr Umfeld definieren und gerade auch ihre Interaktion mit anderen einen relevanten Beitrag zur Formung und Darstellung ihrer Persönlichkeit beiträgt. Für die eigene Selbstdarstellung kann es somit durchaus von Bedeutung sein, in einem sozialen Netzwerk beispielsweise Angaben darüber zu machen, mit welcher anderen Person man etwas unternommen hat und was diese andere Person darüber gedacht hat. Das Übermitteln von Daten über Dritte kann daher nicht nur eine von der Meinungsfreiheit geschützte Tätigkeit sein, sondern auch eine Form der Selbstdarstellung und damit eine Ausübung des allgemeinen Persönlichkeitsrechts.

---

777 So auch *Piltz*, Soziale Netzwerke, S. 110; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 351 ff.; *Dies./Ders.*, ZD 2011, 160 (163); vgl. auch *Buchholtz*, AöR 2015, 121 (138 f.).

778 So auch schon *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 351; *Dies./Ders.*, ZD 2011, S. 160 (163);

779 Im Rahmen der Interessenabwägung nach der DS-GVO wäre hier natürlich auf die korrespondierenden Art. 11 und Art. 7, 8 GrCH abzustellen, vgl. hierzu instruktiv *Chmelik*, Social Network Sites, S. 224 ff.

780 *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 166 ff.; hierzu auch noch ausführlich unter D.III.4.a).

In Ermangelung eines gesetzlichen Erlaubnistatbestands wären derartige Formen der Datenverarbeitung stets nur mit einer Einwilligung der betroffenen Person zulässig. Dies würde eine erhebliche Einschränkung darstellen, da diese Einwilligung regelmäßig nur schwer und umständlich einzuholen ist und jedenfalls eine größere Hürde darstellt als ein gesetzlicher Erlaubnistatbestand in Form einer Interessenabwägung. Es gibt indes keinen verfassungsrechtlichen Grund, die Eingriffsschranken des Rechts auf informationelle Selbstbestimmung gegenüber wirtschaftlichen Interessen und den damit verbundenen Grundrechten der Berufs- und Eigentumsfreiheit enger zu ziehen als gegenüber den persönlichen Entfaltungsfreiheiten anderer Bürger.

Insbesondere ist der Betroffene in beiden Konstellationen ähnlich betroffen: Es werden ohne seine direkte Einwilligung Daten von ihm verarbeitet. Teilweise wird sogar davon ausgegangen, dass das Risiko für die informationelle Selbstbestimmung stets geringer ist, wenn eine Datenverarbeitung zu privaten Zwecken anstatt zu gewerblichen Zwecken durch Unternehmen erfolgt, und die private Datenverarbeitung daher erst Recht zu den erleichterten Bedingungen des § 28 Abs. 1 S. 1 BDSG zu gestatten ist.[781] Dies ist allerdings in dieser Pauschalität eher fraglich. Natürlich können für einen Betroffenen durch eine geschäftsmäßige Datenverarbeitung ernste negative wirtschaftliche Folgen entstehen, etwa wenn ein Versicherungsunternehmen aufgrund bestimmter personenbezogener Daten höhere Prämien berechnet. Allerdings werden geschäftsmäßig verarbeitete Daten häufig intern genutzt und damit anders als bei einer Übermittlung in sozialen Netzwerken nicht veröffentlicht. Die potentielle Verbreitung der Daten und damit auch der negative Effekt für die informationelle Selbstbestimmung kann dadurch bei einer privaten Verarbeitung auch deutlich größer sein.[782] Zwar wären persönliche Schmähkritik, falsche Tatsachen oder Formalbeleidigungen im Zweifel schon nicht als ein berechtigtes Interesse anzusehen, da sie nicht von der Meinungsfreiheit geschützt sind.[783] Die immer wieder stattfindenden „Shitstorms“ sind indes Beispiele dafür, wie auch eine private Datenübermittlung erhebliche Folgen für den Betroffenen haben kann. Ein solcher „Shitstorm“ entzündet sich häufig an im Grundsatz wahren Tatsachen, etwa einer Beschwerde über als unangemessen empfundenes Verhalten, auf die im Folgenden zahlreiche andere Nutzer antworten und sich über das kritisierte Verhalten echauffieren. Zumindest die ursprüngliche, sachgemäße Beschwerde dürfte daher im Regelfall

781 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 353.
782 Vgl. *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 167 f., 190 f.
783 So auch *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 354; *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 231 ff.

von der Meinungsfreiheit geschützt sein.[784] Die aus dem „Shitstorm“ resultierende Verunglimpfung einer Person kann aber massive Folgen haben, anfangen bei einem Ansehensverlust, bis hin zum Jobverlust oder gar Suizidneigung.[785] Darüber hinaus können auch zu privaten Zwecken übermittelte Daten etwa über die Lebensumstände und daraus ableitbar beispielsweise die Kreditwürdigkeit eines Betroffenen von anderen Wirtschaftsteilnehmern zur Kenntnis genommen werden und sich negativ auswirken. Somit kann nicht allgemein davon ausgegangen werden, dass zu privaten Zwecken erfolgende Datenverarbeitung insbesondere in sozialen Netzwerken grundsätzlich weniger risikobehaftet für die informationelle Selbstbestimmung ist als eine Datenverarbeitung zu geschäftlichen Zwecken. Vielmehr ist stets eine differenzierte Einzelfallbetrachtung erforderlich.

Diese einzelfallabhängigen Fragen können indes im Rahmen der konkreten Interessenabwägung berücksichtigt werden. Bis zur Geltung des Art. 6 Abs. 1 lit. f) DS-GVO sind die §§ 28 ff. BDSG daher analog auf eine private Datenverarbeitung durch Nutzer in sozialen Netzwerken anzuwenden.[786]

iv) Zwischenergebnis

Nutzer sozialer Netzwerke sind somit datenschutzrechtlich Verantwortliche, wenn sie personenbezogene Daten Dritter in das soziale Netzwerk einstellen und diese damit an den Anbieter des sozialen Netzwerks übermitteln. Sie unterliegen insoweit datenschutzrechtlichen Pflichten, insbesondere Benachrichtigungs-, Berichtigungs- und Löschungspflichten.

Diese Datenverarbeitung in Form der Übermittlung ist insbesondere dann zulässig, wenn diese gemäß §§ 28 Abs. 1 S. 1 Nr. 2, 29 Abs. 1 Nr. 1 BDSG analog bzw. Art. 6 Abs. 1 lit. f) DS-GVO zur Wahrung der Meinungsfreiheit und des Persönlichkeitsrechts des datenverarbeitenden Nutzers erforderlich ist und die schutzwürdigen Interessen des Betroffenen nicht überwiegen. Die so ermöglichte Interessenabwägung mit klarem gesetzlichen Erlaubnistatbestand schafft Rechtssicherheit und ermöglicht einen verhältnismäßigen Interessen- und Grundrechtsausgleich im Einzelfall. Sie zeigt, dass bereits das geltende Datenschutzrecht flexibel genug ist, um mit der Herausforderung der Datenverarbeitung zu privaten Zwecken durch Nutzer in sozialen Netzwerken umzugehen. Diese Nutzer können zwar trotz des

---

784 Vgl. *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 238.

785 Vgl. *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 78; vgl. zur Wahrnehmung von Online-Mobbing auch *DIVSI*, U25-Studie v. Februar 2014, S. 123 ff.

786 *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 353 f.; *Dies./Ders.*, ZD 2011, S. 160 (163); beschränkt auf eine Veröffentlichung des Profils im gesamten Internet im Ergebnis zustimmend: *Piltz*, Soziale Netzwerke, S. 110 ff.

Haushaltsprivilegs als Verantwortliche für die Übermittlung der Daten eingestuft werden, erhalten aber im Gegenzug auch die gesetzliche Befugnis, im Rahmen einer Interessenabwägung gemäß § 28 Abs. 1 S. 1 Nr. 2 BDSG Daten Dritter ggf. auch ohne deren Einwilligung verarbeiten zu dürfen.

Für das hierüber hinausgehende Problem des Direkterhebungsgrundsatzes gemäß § 4 Abs. 2 BDSG gilt das oben unter D.I.3.a)cc) Gesagte.

cc) Nutzer als „Diensteanbieter" im Sinne des TMG

Nutzer sozialer Netzwerke können darüber hinaus unter bestimmten Umständen als Diensteanbieter im Sinne von § 2 Nr. 1 TMG angesehen werden. Sie unterliegen dann nicht nur einschlägigen datenschutzrechtlichen, sondern zudem telemedienrechtlichen Pflichten. Auch hier zeigt sich somit die Umwandlung des bipolaren Anbieter-Nutzer Verhältnisses in komplexere, mehrseitige Rechtsbeziehungen, die das Internet im Allgemeinen und soziale Netzwerke mit sich bringen. Da die DS-GVO die telemedienrechtlichen Regelungen, die auf der ECRL und den zugehörigen Richtlinien zur Regelung der elektronischen Kommunikation beruhen, unberührt lässt, wird die konkrete Einordnung der Nutzer als Diensteanbieter auch in Zukunft relevant bleiben, insbesondere mit Blick auf die unten diskutierte Frage nach einer möglichen Impressumspflicht.[787]

Wann ein angebotenes Telemedium vorliegt – und damit indirekt auch die Eigenschaft als Diensteanbieter nach § 2 Nr. 1 TMG –, wird in § 1 Abs. 1 TMG vor allem durch negative Abgrenzung festgelegt, es gibt keine Legaldefinition. Die Gesetzbegründung stellt insbesondere auf wirtschaftliche Tätigkeiten ab, die elektronisch in Form von Bild-, Text- oder Toninhalten zur Verfügung gestellt werden, wobei es auf die Entgeltlichkeit des Angebots nicht ankommt.[788] Ein angebotenes Telemedium im Sinne der Vorschrift liegt nach ganz herrschender Ansicht bereits dann vor, wenn beispielsweise auf einer Internetplattform ohne weitere Interaktionsmöglichkeiten für Waren geworben wird.[789] Eine Kontrolle des Anbieters über die Serverstrukturen ist nicht erforderlich, solange er den Inhalt des Angebots selbst bestimmen kann, dieses mithin kommunikativ eigenständig ist.[790] Aus der Einstufung als

[787] Unten unter D.II.1.

[788] BT-Drs. 16/3078, S. 13; *Ricke*, in: Spindler/Schuster, § 1 TMG, Rn. 11, § 2 TMG, Rn. 2.

[789] OLG Düsseldorf, K&R 2013, 594 (595), Rn. 28; OLG Düsseldorf, MMR 2008, 682 (683); OLG Frankfurt, CR 2007, 454 (454); *Ricke*, in: Spindler/Schuster, § 2 TMG, Rn. 2 m.w.N.

[790] Dazu oben unter D.I.2; vgl. zum Kriterium der „kommunikationsbezogenen Eigenständigkeit" im Rahmen von Plattformangeboten: OLG Düsseldorf, K&R 2013, 594 (595), Rn. 28; *Ricke*, in: Spindler/Schuster, § 2 TMG, Rn. 2.

Diensteanbieter können erhebliche Pflichten folgen, insbesondere im Falle von geschäftsmäßig angebotenen Telemedien eine Impressumspflicht gemäß § 5 Abs. 1 TMG[791], aber auch die datenschutzrechtlichen Verpflichtungen gemäß §§ 11 ff. TMG. Gerade letztere werden freilich unter der Geltung der DS-GVO formal nur noch von der Einstufung als allgemein Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO abhängig sein, soweit nur noch auf Art. 6 DS-GVO für die Rechtmäßigkeit einer Datenverarbeitung abzustellen ist. Sollte indes zur Bildung von Fallgruppen faktisch weiterhin auf die Regelungen der §§ 11 ff. TMG zurückgegriffen werden, bleibt konsequenterweise auch die Frage relevant, unter welchen Voraussetzungen Nutzer als Diensteanbieter einzuordnen sind.

Im Rahmen von sozialen Netzwerken muss hierbei unterschieden werden erstens zwischen Profilen, die ausdrücklich der Verfolgung kommerzieller Interessen dienen, zweitens rein privaten Zwecken genutzten Profilen und drittens gemischt-genutzten Profilen insbesondere in beruflich orientierten sozialen Netzwerken wie Xing oder LinkedIn.

i) Kommerziellen Interessen dienende Profile

Werbung für Waren und Dienstleistungen erfolgt zunehmend über Profile in sozialen Netzwerken. Diese Werbung kann einerseits über persönliche Profile erfolgen, andererseits aber auch über speziell für Unternehmen eingerichtete Seiten. Facebook, aber auch z.B. Google Plus, bietet beispielsweise explizit die Möglichkeit an, sogenannte „Fanpages" zu erstellen, auf denen für Dienstleistungen und Produkte oder das ganze Unternehmen an sich geworben werden kann.[792] Hierbei nimmt der Anbieter des sozialen Netzwerks zwar einen gewissen Einfluss auf die inhaltliche Gestaltung des Profils, indem durch die Eingabemasken und die Nutzungsbedingungen bestimmt wird, welche Angaben überhaupt möglich sind.[793] Diese Einflussnahme ist indes zu gering, um dem Profilersteller die Kontrolle über die inhaltliche Gestaltung abzusprechen, zumindest solange die Eingabemasken hinreichend abstrakt bleiben, um eine individuelle, inhaltliche Gestaltung zu ermöglichen. Soziale Netzwerke dienen per definitionem als Plattform für die Selbstdarstellung der Nutzer. Der gemeinsame Rahmen und die einheitliche Gestaltung hat keine Bedeutung für den wahrgenommenen Inhalt. Aus der

791 LG Aschaffenburg, MMR 2012, 38 (39); *Pießkalla*, ZUM 2014, S. 368 (370); *Richter*, MMR 2014, S. 517 (518); *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 81 ff.; zustimmend auch *Piltz*, Soziale Netzwerke, S. 102 f., 106 f., allerdings nur mit der vagen Feststellung begründet, Unternehmer hätten „mehr Einfluss auf die Gestaltung ihrer Seite" und „eine freie Entfaltungsmöglichkeit", anders als privat agierende Verbraucher, denen als „Thema" eine „Nutzung zu privaten Zwecken [vorgegeben]" werde (a.a.O., S. 107).

792 *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (123 f.); *Lichtnecker*, GRUR 2013, 135 (136 ff.).

793 *Lorenz*, VuR 2014, S. 83 (86); *Jandt/Roßnagel*, ZD 2011, 160 (162); *Lichtnecker*, GRUR 2013, 135 (136).

Perspektive eines verständigen Dritten dürfte daher klar sein, dass es sich bei derartigen Fanpages um einen kommunikativ eigenständigen Internetauftritt des Profilinhabers im Rahmen der Plattform handelt und nicht um ein Angebot des Anbieters des sozialen Netzwerks.[794] Es wäre eine arg künstliche Aufspaltung, bei einer einheitlichen Verkaufsplattform wie eBay die Diensteanbietereigenschaft der Nutzer zu bejahen, in einem sozialen Netzwerk für ggf. dasselbe Angebot auf einer Fanpage aber zu verneinen. Profilseiten, die zu geschäftlichen Zwecken unterhalten werden – mithin insbesondere Fanpages –, stellen daher kommunikativ eigenständige Angebote dar, mit der Folge, dass der Profilinhaber als Diensteanbieter einzustufen ist.[795]

ii) Ausschließlich zu privaten Zwecken genutzte Profile

Problematischer ist, ob auch solche Nutzer als Diensteanbieter zu qualifizieren sind, die lediglich ein persönliches Profil zu privaten Zwecken in einem sozialen Netzwerk haben und anderen Nutzern hierauf Zugriff gewähren. Da eine persönliche, private Nutzung für juristische Personen nicht in Betracht kommt, kann es sich hierbei nur um Profile natürlicher Personen handeln.[796] Die Gesetzesbegründung zu § 1 Abs. 1 TMG stellt ausdrücklich auf „einen weiten Bereich wirtschaftlicher Tätigkeiten“ (Hervorhebung der Verfasserin) ab, die von dem Begriff der Telemedien erfasst sind.[797] Die nachfolgend aufgezählten Beispiele der Gesetzesbegründung, nämlich u.a. Onlineangebote von Waren und Dienstleistungen, Videos auf Abruf, Internetsuchmaschinen und Werbe-Emails, weisen keinerlei Bezug zu rein privaten und persönlichen Tätigkeiten auf. Dem steht indes die Gesetzesbegründung zu § 5 Abs. 1 TMG gegenüber, welche auch ausdrücklich private Angebote wie eine persönliche Webseite als Telemedium bezeichnet und speziell gewerbsmäßige Angebote hiergegen abgrenzt.[798]

---

794 *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (123); *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 81; *Ricke*, in: Spindler/Schuster, § 2 TMG, Rn. 2; *Rockstroh*¸ MMR 2013, 627 (628 f.); jedenfalls implizit wohl auch *Lichtnecker*, GRUR 2013, 135 (136); a.A. *Lorenz*, VuR 2014, S. 83 (86); *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 350, allerdings nur mit einem pauschalen Verweis auf „regelmäßig thematische und einheitliche gestalterische Vorgaben“ durch soziale Netzwerke und ohne spezifisch auf Fanpages einzugehen.

795 LG Aschaffenburg, MMR 2012, 38 (39); LG Regensburg, CR 2013, 197 (197); VG Schleswig, ZD 2014, 51 (52); *Ricke*, in: Spindler/Schuster, § 2 TMG, Rn. 2; *Pießkalla*, ZUM 2014, S. 368 (370); *Richter*, MMR 2014, 517 (518); *Rockstroh*¸ MMR 2013, 627 (629); *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (123); *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 81 ff.; *Piltz*, Soziale Netzwerke, S. 102 f., 106 f.; *Hullen/Roggenkamp*, in: Plath, § 11 TMG Rn. 7; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 17 f.; A.A. *Lorenz*, VuR 2014, S. 83 (86); *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 350.

796 Vgl. *Rockstroh*¸ MMR 2013, 627 (630).

797 BT-Drs. 16/3078, S. 13.

798 BT-Drs. 16/3078, S. 14.

Anders als bei kommerziell genutzen Fanpages ist allerdings der kommunikativ eigenständige Gehalt eines privat genutzten Profils in einem sozialen Netzwerk vernachlässigbar gering. Freilich präsentiert sich ein Nutzer individuell und gestaltet sein Profil insoweit selbstständig; die Übermittlung derartiger Inhalte ist indes auch der Kern des sozialen Netzwerks an sich. Es werden keine Dienstleisung und kein Produkt angeboten, die sich in irgendeiner Form von dem Diensteangebot des Anbieters des sozialen Netzwerks unterscheiden würden.[799] Konsequenterweise ist daher bei ausschließlich privat genutzten Nutzerprofilen in sozialen Netzwerken bereits die eigenständige Telemedienqualität im Sinne des § 1 Abs. 1 TMG zu verneinen, so dass derartige Nutzer nicht als Diensteanbieter im Sinne von § 2 Nr. 1 TMG zu qualifizieren sind.[800]

Soweit vereinzelt dennoch eine Eigenschaft als Diensteanbieter bejaht wird, erwachsen hieraus jedenfalls keine praktischen Konsequenzen, da den Nutzern mangels einer Gewerbsmäßigkeit des Angebots keine Impressumspflicht aus § 5 Abs. 1 TMG zukommt[801] und mangels einer hinreichenden Einflussmöglichkeit und Kontrolle über die erhobenen Daten auch nicht vorstellbar ist, dass es zu Pflichten nach den §§ 7 ff. TMG und §§ 11 ff. TMG kommen könnte.

iii) Gemischt-genutzte Profile insbesondere in beruflich orientierten sozialen Netzwerken

Zwischen ausdrücklich kommerziell genutzten Fanpages und ausschließlich privat genutzten Profilen existiert schließlich der Graubereich persönlicher Profile in überwiegend beruflich orientierten sozialen Netzwerken wie Xing oder Linked-In oder vergleichbar genutzter Fanpages bei Facebook. Anders als bei rein privaten Profilen, die der Selbstdarstellung im privaten und persönlichen Kreis dienen, verfolgen diese Profile auch wirtschaftliche Zwecke wie die Kundenakquise (z.B. bei Maklern, Anwälten oder Beratern) oder eine Bewerbung um eine neue Arbeitsstelle als Förderung der eigenen wirtschaftlichen Betätigung.[802] Auch ohne eine direkte Möglichkeit zur Bestellung oder Buchung entsprechender Dienstleistungen

---

799 So auch bereits *Piltz*, Soziale Netzwerke, S. 107.

800 So *Ricke*, in: Spindler/Schuster, § 2 TMG, Rn. 2; *Piltz*, Soziale Netzwerke, S. 107; a.A. *Pießkalla*, ZUM 2014, S. 368 (370); *Richter*, MMR 2014, S. 517 (518). Eine gelegentlich über das Profil getätigte Empfehlung an Freunde für Bücher, Musik oder sonstige Dienstleistungen und Waren ist in der dieser Hinsicht unschädlich, solange nicht die Schwelle zu einer wirtschaftlichen Tätigkeit überschritten wird. Dies wird in aller Regel bereits deswegen nicht der Fall sein, weil der die Empfehlung aussprechende Nutzer regelmäßig keinen wirtschaftlichen Vorteil von dieser Empfehlung hat. Selbst wenn der Nutzer im Einzelfall eine kleine Belohnung von einem Unternehmen bekommt, wenn er erfolgreich mit seiner Empfehlung einen neuen Kunden wirbt, stellt dies regelmäßig noch keine gewerbsmäßige Tätigkeit dar.

801 So *Pießkalla*, ZUM 2014, S. 368 (370); *Richter*, MMR 2014, S. 517 (518); vgl. auch *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 83; ausführlich zur Frage einer Impressumspflicht gemäß § 55 Abs. 1 RStV und dem möglichen Spannungsverhältnis zu § 13 Abs. 6 TMG noch unten unter D.II.1.

802 *Pießkalla*, ZUM 2014, S. 368 (370).

erscheint es konsequent, jedenfalls für Profilinhaber, deren Profile der Kundenakquise dienen können, eine wirtschaftliche Tätigkeit und damit eine Einstufung als Diensteanbieter zu bejahen, selbst wenn man einen wirtschaftlichen Bezug hierfür fordert.[803] Da die Tätigkeit regelmäßig auch geschäftsmäßig sein wird, besteht entsprechend eine Impressumspflicht nach § 5 Abs. 1 TMG.[804]

Das Angebot der eigenen, potentiellen Arbeitskraft im Rahmen eines Bewerbungsprofils z.B. auf Xing dient hingegen allenfalls der Vorbereitung späterer wirtschaftlicher Tätigkeiten, stellt aber selbst keine solche dar. Insoweit ist jedenfalls eine Impressumspflicht mangels einer Geschäftsmäßigkeit zu verneinen.[805] Damit entfällt zumindest eine sehr maßgebliche Konsequenz, wenn man das Betreiben eines solchen Bewerberprofils als telemedienrechtliches Diensteangebot einstuft.

In einer sehr strikten Abgrenzung von beruflicher und privater Sphäre sind derartige Bewerbungsprofile trotz des nur vorbereitenden Charakters einer späteren wirtschaftlichen Tätigkeit der wirtschaftlich-beruflichen Sphäre zuzuteilen. Weder aus dem Gesetz noch aus der Gesetzesbegründung lässt sich indes mit letztgültiger Sicherheit schließen, ob es sich tatsächlich um ein Diensteangebot handelt. Dies ist maßgeblich darauf zurückzuführen, dass das Angebot der individuellen Arbeitskraft und -bereitschaft einen signifikanten qualitativen Unterschied gegenüber dem vom Gesetzgeber anvisierten Diensteangebot an eine breite Masse aufweist: Das Angebot der individuellen Arbeitskraft richtet sich ebenso wie das Angebot einer Dienstleistung oder Ware an einen im Prinzip offenen Adressatenkreis, die diese Leistung nachfragen können. Andererseits handelt es sich aber auch um ein exklusives Angebot, das letztlich nur in einem Fall angenommen werden kann. Die Interessen- und Gefährdungslage der Beteiligten ist dadurch anders als bei einem regelmäßigen Vertrieb von Waren oder Dienstleistungen.

Vorzugswürdig scheint dennoch, um der Schaffung von Rechtssicherheit willen, eine klare Abgrenzung anhand der verobjektivierten wirtschaftlichen oder privaten Nutzungsintention

---

803 Möglichkeiten für eine Kundenakquise bestehen z.B. insbesondere dann, wenn in einem solchen Profil für die eigene Dienstleistung geworben wird und eine Kontaktadresse angegeben ist. Die gezielte Selbstdarstellung als Makler, Anwalt, Berater oder Ähnliches informiert potentielle Kunden in dem Netzwerk bereits hinreichend über die Tätigkeit, um einen späteren Vertrag bei entsprechendem Interesse anzubahnen. Ausschließlich auf die Möglichkeit zur direkten Bestellung oder Buchung der Dienstleistung über das soziale Netzwerk abzustellen, erweist sich daher angesichts zahlreicher alternativer Kommunikationsmethoden als zu eng.

804 *Rockstroh*¸ MMR 2013, 627 (629 f.); ausführlich zur Impressumspflicht unten unter D.II.

805 A.A. *Pießkalla*, ZUM 2014, S. 368 (370).

vorzunehmen und daher auch solche Bewerbungsprofile als Diensteangebot und die sie verwendenden Nutzer entsprechend als Diensteanbieter gemäß § 2 Nr. 1 TMG einzustufen.[806]

dd) Zwischenergebnis: Datenschutzrechtliche Verantwortlichkeit der Nutzer sozialer Netzwerke

Die vorstehende Analyse hat gezeigt, dass Nutzer sozialer Netzwerke datenschutzrechtlich verantwortlich sind, soweit sie selbst personenbezogene Daten über Dritte in dem sozialen Netzwerk übermitteln. Sie unterliegen nicht dem Haushaltsprivileg des § 1 Abs. 2 Nr. 3 BDSG bzw. Art. 2 Abs. 2 lit. c) DS-GVO, so dass das Datenschutzrecht vollumfänglich anwendbar ist. Mangels ausdrücklicher Erlaubnistatbestände im Gesetz für eine Datenverarbeitung zu privaten Zwecken sind die §§ 28, 29 BDSG analog anzuwenden. Mit Anwendbarkeit des Art. 6 DS-GVO wird dieses Problem entfallen, da dieser insbesondere in Abs. 1 lit. f) die berechtigten Interessen nicht länger auf einen geschäftlichen Kontext limitiert und damit auch rein private Interessen ausdrücklich erfasst sind.

Die Nutzer sind darüber hinaus als Diensteanbieter i.S.v. § 2 Nr. 1 TMG anzusehen, soweit sie mit ihren Profilen wirtschaftliche Tätigkeiten ausüben. Ist die Tätigkeit zudem geschäftsmäßig, unterliegen sie einer Impressumspflicht gemäß § 5 Abs. 1 TMG. Dies führt freilich zu Konflikten mit dem Recht auf anonyme Nutzung gemäß § 13 Abs. 6 TMG, die ausführlich unten unter D.II.2 besprochen werden.

Soweit sie als Diensteanbieter anzusehen sind, unterliegen sie zudem gegenwärtig noch den datenschutzrechtlichen Verpflichtungen der §§ 11 ff. TMG. Gemäß § 12 Abs. 3 TMG i.V.m. § 3 Abs. 7 BDSG müssten sie allerdings zusätzlich datenschutzrechtlich Verantwortliche sein, um im Umgang mit von ihnen erhobenen und verarbeiteten Bestands- und Nutzungsdaten an die Vorgaben des TMG gebunden zu sein. In diesem Fall sind sie unter anderem Adressaten des Auskunftsanspruchs anderer Nutzer gemäß § 13 Abs. 7 TMG hinsichtlich der von ihnen gespeicherten Daten.[807] Indem mit der DS-GVO die §§ 11 ff. TMG aller Voraussicht nach

806 Vgl. auch *Pießkalla*, ZUM 2014, S. 368 (370).

807 Ob sich diese Verantwortlichkeit in der Praxis überhaupt auswirkt, ist indes sehr fraglich. Den entsprechenden Profilinhabern kommt zwar die inhaltliche Gestaltungshoheit über die Seiten zu, die somit kommunikativ eigenständig sind, was zu ihrer Eigenschaft als Diensteanbieter führt. Die technische Seite der Datenerhebung und -verarbeitung liegt dagegen in aller Regel in der Hand des Plattformanbieters. Dieser kontrolliert entsprechend auch primär die Zwecke und Mittel der Datenverarbeitung und ist somit datenschutzrechtlich Verantwortlicher gemäß § 3 Abs. 7 BDSG, auf den gemäß § 12 Abs. 3 TMG abzustellen ist. Insofern ist sehr zweifelhaft, ob für die Profilinhaber überhaupt jemals die Möglichkeit oder das Bedürfnis nach der eigenen Erhebung und Verarbeitung von Bestands- und Nutzungsdaten entsteht, was aber Voraussetzung für das Bestehen eigener datenschutzrechtlicher Pflichten gemäß §§ 11 ff. TMG wäre.

verdrängt werden[808], wird diese Aufteilung der datenschutzrechtlichen Verantwortlichkeit auf verschiedene Gesetze zugunsten einer größeren Rechtsklarheit beendet.

Ein besonderes Problem liegt aber nach gegenwärtigem und auch zukünftigem Recht in der Frage, ob den Anbietern von Fanpages über die Verantwortlichkeit für die eigene Datenverarbeitung hinaus auch eine Verantwortlichkeit für die Datenverarbeitung durch den Anbieter des sozialen Netzwerks zukommt. Dieser Frage soll nun im Folgenden nachgegangen werden.

c) Verantwortlichkeit der Betreiber von „Fanpages"

Bei Facebook und Google Plus haben Nutzer nicht nur die Möglichkeit, sich ein privates, persönliches Profil anzulegen. Sie können auch sogenannte „Fanpages" erstellen. Im Gegensatz zu persönlichen Profilen erlauben sie eine unbegrenzte Zahl an „Followern" bzw. bei Facebook Nutzern, denen das „gefällt".[809] Sie werden regelmäßig zur Selbstdarstellung von Unternehmen, Marken, öffentlichen Personen, Vereinen oder Ähnlichem verwendet. Durch die Einbindung in das soziale Netzwerk ist eine große Verbreitungsmöglichkeit gewährleistet, ohne dass das Unternehmen selbst in eine Mitgliederverwaltung investieren müsste, wie dies etwa bei einem Newsletter der Fall wäre.[810] Fanpages stellen für Unternehmen somit sehr kostengünstige und zugleich effiziente Werbeplattformen dar.[811] Die hohe Reichweite ergibt sich neben der abstrakt hohen Nutzerzahl insbesondere Facebooks vor allem daraus, dass Facebook Aktivitäten einzelner Nutzer auf Fanpages auch möglicherweise interessierten Kontakten dieser Nutzer anzeigt. Hierdurch werden weitere Nutzer auf das Angebot der Fanpage aufmerksam gemacht. Dieses Verbreiten der Aktivitäten auf der Fanpage beruht auf der Auswertung von Nutzerprofilen und einer Zusammenführung mit den im Rahmen eines Fanpage-Besuchs anfallenden Bestands- und Nutzungsdaten.[812] Dem Betreiber einer Fanpage wird zudem über die Funktion „Facebook Insights" die Möglichkeit geboten, anonymisierte Statistiken über die Nutzer der Fanpage zu erhalten und sein Angebot damit noch zielgruppengerechter zu präsentieren.[813]

---

808 Vgl. hierzu bereits ausführlich oben unter C.I.2.
809 *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 68.
810 *Lichtnecker*, GRUR 2013, 135 (136).
811 *Lichtnecker*, GRUR 2013, 135 (135 f.); vgl. auch *Hoffmann-Riem*, Innovation und Recht, S. 625 f.
812 Vgl. *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (3); *Lichtnecker*, GRUR 2013, 135 (136); *Karg/Thomsen*, DuD 2012, 729 (731).
813 *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (123); *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 68 ff.; *Karg/Thomsen*, DuD 2012, 729 (731).

Fanpages sind innerhalb des sozialen Netzwerks öffentlich einsehbar und häufig sogar vergleichbar mit einer „normalen" Webseite aufrufbar und über Suchmaschinen auffindbar. Ein Besucher muss in dem sozialen Netzwerk daher weder eingeloggt noch überhaupt registriert sein, sondern kann die Seite direkt öffnen. Fanpages richten sich daher nicht nur an die Mitglieder des sozialen Netzwerks, sondern potentiell die gesamte Internetöffentlichkeit. Selbst nach der weitesten Auffassung fallen sie daher nicht unter das Haushaltsprivileg. Auch die von anderen Nutzern getätigten Kommentare können in der Regel öffentlich eingesehen werden. Lediglich um selbst aktiv die Kommentarfunktion nutzen zu können, muss sich ein Nutzer zunächst mit seinem Account in dem sozialen Netzwerk einloggen.

Zudem stellen sie in aller Regel selbstständige inhaltliche Angebote gegenüber dem allgemeinen sozialen Netzwerk dar. Wie im vorigen Abschnitt dargelegt wurde, sind die hinter einer Fanpage stehenden Nutzer daher regelmäßig als „Diensteanbieter" im Sinne von § 2 Nr. 1 TMG einzustufen, sofern die mit der Fanpage beworbenen Inhalte als wirtschaftliche Tätigkeit eingestuft werden können.[814] Ihnen kommen entsprechend Pflichten gemäß dem TMG zu. Diese können insbesondere eine Impressumspflicht nach § 5 Abs. 1 TMG umfassen. Problematisch und heftig umstritten ist dagegen, in welchem Umfang datenschutzrechtliche Pflichten gemäß §§ 11 ff. TMG bzw. den sie zukünftig ersetzenden Vorschriften der DS-GVO für durch den Anbieter des sozialen Netzwerks erhobene und verarbeitete Bestands- und Nutzungsdaten bestehen.

Im Hinblick auf die Verantwortlichkeit für Inhaltsdaten gemäß dem BDSG gilt dagegen das für Nutzer allgemein Festgestellte: Soweit Fanpage-Betreiber auf ihrer Fanpage selbst personenbezogene Daten über Dritte übermitteln, speichern oder auf andere Weise verarbeiten, sind sie hierfür datenschutzrechtlich verantwortlich.[815]

Außen vor bleiben im Folgenden die Fragen nach der zivilrechtlichen Haftung auf Schadensersatz wegen Persönlichkeits- oder Urheberrechtsverletzungen und Ähnlichem.[816]

---

814 Ausführlich oben unter D.I.3.b)cc).

815 ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 17; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 10 f.; vgl. auch schon oben unter D.I.3.b)bb). Anders als die Anbieter sozialer Netzwerke sind Fanpage-Betreiber allerdings nicht für nutzergenerierte Inhaltsdaten verantwortlich, die von anderen Nutzern auf der Fanpage generiert werden (vgl. zur Anbieterverantwortlichkeit insoweit oben unter D.I.3.a)aa)). Sie haben keinen vergleichbaren Einfluss auf die Generierung dieser Daten und sie erheben und verwenden diese auch nicht selbst zur Erstellung von Persönlichkeitsprofilen, so dass es an dem wirtschaftlich-funktionellen Zusammenhang und entsprechend einer Kontrolle über die Zwecke und Mittel der Datenverarbeitung fehlt.

816 Hierzu *Hoeren*, in: Ders./Sieber/Holznagel, Hdb. Multimediarecht, Teil 18.2, Rn. 60 ff., 121 ff.

aa) Datenschutzverstöße durch Facebook im Zusammenhang mit Bestands- und Nutzungsdaten beim Besuch von Fanpages

Wie oben in Kapitel C.II herausgearbeitet, ist jedenfalls unter Berücksichtigung der EuGH Entscheidung zu *Google Spain*[817] richtigerweise davon auszugehen, dass in Deutschland deutsches Datenschutzrecht auf Facebook Anwendung findet. Hiervon ausgehend soll im Folgenden eine kurze, exemplarische Analyse erfolgen, inwieweit Facebook insbesondere im Rahmen der Erhebung und Verwendung von Bestands- und Nutzungsdaten der Nutzer beim Besuch von Fanpages gegen geltendes Datenschutzrecht verstößt und ob diese Verstöße auch nach der DS-GVO bestehen bleiben. Diese Untersuchung verfolgt freilich einen selektiven Ansatz, da neben dem Datenschutzrecht unter anderem auch Verstöße gegen Wettbewerbsrecht und AGB-Recht durch die Verbraucher benachteiligende Klauseln in den Nutzungsbestimmungen oder Datenrichtlinien durch Facebook im Raum stehen. Um den Rahmen dieser Arbeit nicht zu sprengen, sollen diese Fragen hier allerdings ausgeklammert und soll nur auf entsprechende zivilrechtliche Analysen[818] und Gerichtsentscheidungen[819] verwiesen werden.

Die einschlägigen Regelungen für die Rechtmäßigkeit der Erhebung und Verwendung von Bestands- und Nutzungsdaten folgen aus den §§ 11 ff. TMG bzw. zukünftig Art. 6 DS-GVO.[820] Um eine rechtliche Analyse zu ermöglichen, ist es einmal mehr erforderlich, sich zunächst die technischen Abläufe beim Aufruf von Fanseiten und die darauf folgende Datenverarbeitung grob vor Augen zu führen.

Mit dem Aufruf der Fanpage erhält Facebook zunächst die IP-Adresse des Nutzers, um den Inhalt der Fanpage auf dessen Endgerät darstellen zu können.[821] Gleichzeitig werden weitere Bestands- und Nutzungsdaten erhoben und gespeichert, um den Dienst überhaupt zu ermöglichen, so etwa Login-Daten. Zudem werden durch Cookies weitere Daten an Facebook übertragen. Bei nicht-eingeloggten Internetnutzern geschieht dies vor allem über den datr-Cookie, welcher beim Besuch der Domäne facebook.com, auf der auch die Fanseite liegt,

817 EuGH, *Google Spain*, Rs. C-131/12, Rn. 28, 37, 80 = JZ 2014, 1009 ff.

818 *Wauters, u.a.*, Internat. J. of Law and Inf. Tech., 2014 (22), 254 (263 ff.); *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 45 ff.; *Piltz*, Soziale Netzwerke, S. 34 ff., 244 ff.

819 In mehreren Verfahren wurden bereits AGB-Klauseln von Facebook für rechtswidrig und unwirksam erklärt, vgl. LG Berlin, ZD 2012, 276 (278 ff.); KG Berlin, ZD 2014, 412 (417 ff.); LG Berlin, ZD 2015, 133 (134 ff.).

820 Hierzu oben unter C.I.2 und C.III.

821 *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, S. 404; *Voigt/Alich*, NJW 2011, 3541 (3541).

gesetzt wird und eine spezielle Browseridentifikation an Facebook sendet. Auch wenn der Personenbezug einer dynamischen IP-Adresse noch nicht höchstrichterlich geklärt ist[822], ist im Zusammenspiel mit den weiteren, zeitgleich gespeicherten Daten wie der Browseridentifikation insgesamt von einer Personenbeziehbarkeit auszugehen. Auch bei dem datr-Cookie, der faktisch eine allgemeine Nutzer-ID darstellt, ist davon auszugehen, dass dieser personenbezogene Daten übermittelt und eine Reidentifizierung des jeweiligen Nutzers (bzw. seines Browsers) ermöglicht.[823]

Bei eingeloggten Mitgliedern Facebooks werden über weitere Cookies, z.B. den c_user Cookie, noch detailliertere Informationen über das Nutzerverhalten auf der Fanpage übertragen. Diese sind in jedem Fall als personenbezogene Daten zu werten, da sie von Facebook über das Nutzerprofil ohne weiteres einem individuellen Nutzer zugeordnet werden können.[824] Facebook kann somit eine Reichweitenanalyse über den die Fanpage aufrufenden Nutzer durchführen und die daraus gewonnenen Daten zur weiteren Profilbildung verwenden.[825] Zumindest bei eingeloggten Facebook-Mitgliedern wird die Darstellung der Inhalte der Fanpage zudem an das individuelle Nutzerprofil angepasst.[826]

Facebook registriert darüber hinaus über Cookies und eine Auswertung von Bestands- und Nutzungsdaten, welche Nutzer wie häufig und wie lange auf Fanpages verweilen. Diese Daten werden verwendet, um eine detaillierte Nutzerstatistik zu erstellen, die nach Merkmalen wie Geschlecht, Alter, persönlichen Interessen und nationaler Herkunft aufgeschlüsselt ist.[827] Diese wird in anonymisierter Form den Betreibern der Fanpages – wie auch allgemein

---

822 Der BGH hat diese Frage dem EuGH im Oktober 2014 zur Vorabentscheidung vorgelegt, BGH, ZD 2015, 80 (80 ff.); vgl. auch bereits oben unter C.III.4.c).

823 *Karg/Thomsen*, DuD 2012, 729 (731); Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 19 ff.; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 15, 24 f.; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 7 f.; *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 89 ff.; ein belgisches Gericht erklärte zudem am 9.11.2015 die Setzung des datr-Cookies und die damit einhergehende Datensammlung bei Nichtnutzern für rechtswidrig und verhängte bei Missachtung eine Geldstrafe von 250.000€ pro Tag, vgl. http://www.heise.de/newsticker/meldung/Belgisches-Gericht-Facebook-darf-keine-Daten-von-Nicht-Mitgliedern-sammeln-2912586.html; vgl. auch schon oben unter B.II.2.b)aa). Facebook hat daraufhin angekündigt, den öffentlichen Zugriff für nichtangemeldete Nutzer auf Fanpages in Belgien vollständig zu sperren, um so auch das Setzen des datr-Cookies zu vermeiden, ZD-Aktuell 2015, 04924.

824 AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 15, 25.

825 ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 5 ff.; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 7 ff.; *Voigt/Alich*, NJW 2011, 3541 (3541); vgl. zum Tracking allgemein auch bereits oben unter B.II.2.b).

826 AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 25.

827 ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 12 ff.; *Caspar*¸ ZD 2015, 12 (13).

Werbetreibenden – als sogenanntes „Facebook Insights“ kostenlos zur Verfügung gestellt, um ihr Angebot noch besser auf ihre jeweiligen Zielgruppen ausrichten zu können.[828] Eine Erstellung dieser Statistik setzt aber offensichtlich voraus, dass zuvor die bloß technischen Bestands- und Nutzungsdaten mit den entsprechenden personenbezogenen Daten durch Facebook zusammengeführt werden.

Gemäß § 12 Abs. 1 TMG dürfen personenbezogene Daten zur Bereitstellung von Telemedien nur erhoben und verwendet werden, soweit dies durch Gesetz gestattet ist oder eine Einwilligung vorliegt. Zudem sind in den §§ 13 ff. TMG besondere Regelungen für die Verarbeitung von Bestands- und Nutzungsdaten normiert. Diese werden durch die Art. 12 bis 14 DS-GVO und den Art. 6 DS-GVO weitgehend, wenngleich häufig weniger detailliert und bereichsspezifisch beibehalten.[829] Nach diesen Maßstäben sind mehrere Datenschutzverstöße durch Facebook festzustellen.[830]

i) Tracking von (Nicht-)Nutzern im Internet mit Hilfe des datr-Cookies

Im Rahmen der Tracking-Methoden Facebooks wurde bereits die Funktionsweise des datr-Cookies im Zusammenspiel mit Social PlugIns, speziell dem Like-Button, erläutert.[831] An dieser Stelle soll ein besonderes Augenmerk darauf gerichtet werden, dass Facebook einerseits systematisch ein Opt-Out aus dem Tracking erschwert und andererseits den datr-Cookie auch gegenüber Nichtnutzern einsetzt. Hierdurch werden zusätzliche Daten erhoben, die Facebook nutzen kann, um Persönlichkeitsprofile zu erstellen und damit auch Facebook Insights weiter

---

828 *Karg/Thomsen*, DuD 2012, 729 (731); *Maisch*, Informationelle Selbstbestimmung, S. 209; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 17; ohne spezifisch auf Insights einzugehen, erklärt Facebook hierzu in seinen Datenrichtlinien: „Wir können diesen Partnern Informationen über die Reichweite und Wirksamkeit ihrer Werbung zur Verfügung stellen, ohne Informationen bereitzustellen, mit denen du persönlich identifiziert werden kannst, oder wenn wir die Informationen zusammengefasst haben, so dass sie dich nicht persönlich identifizieren. Beispielsweise können wir Werbetreibenden sagen, wie erfolgreich ihre Werbeanzeigen sind oder wie viele Personen ihre Werbeanzeigen aufgerufen oder eine App installiert haben, nachdem sie eine Werbeanzeige gesehen haben, oder wir können diesen Partnern nichtpersonenbezogene demografische Informationen (wie z. B. eine 25 Jahre alte Frau in Madrid, die sich für Software Engineering interessiert) bereitstellen, damit sie ihre Zielgruppe bzw. ihre Kunden besser verstehen; allerdings erst, nachdem sich die Werbetreibenden zur Einhaltung unserer Richtlinien für Werbetreibende verpflichtet haben.“, https://www.facebook.com/privacy/explanation (Stand 29. September 2016).

829 Ausführlich *Keppeler*, MMR 2015, 779 (781 f.).

830 Vgl. *Weichert*, JBÖS 2012/2013, 379 (380); am 2. März 2016 gab das Bundeskartellamt bekannt, ein Verfahren gegen Facebook aufgrund eines möglichen Verstoßes gegen Datenschutzvorschriften in den Nutzungsbedingungen eingeleitet zu haben, http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568.

831 Vgl. oben unter B.II.2.b)aa).

zu präzisieren. Soweit es hierfür keine gesetzliche Erlaubnis gibt und dies ohne die Einwilligung der Betroffenen erfolgt, ist dies indes rechtswidrig.

Eine Studie des Interdisciplinary Centre for Law and Information and Communication Technology (ICLI/ICT) der KU Leuven, erstellt in Zusammenarbeit mit belgischen, niederländischen und deutschen Datenschutzbehörden, zeigt zunächst, dass unter anderem der datr-Cookie und der fr-Cookie auch dann auf einem Endgerät gespeichert bleiben, wenn sich ein Nutzer explizit bei Facebook ausloggt und in den Konto-Einstellungen angibt, nicht getrackt werden zu wollen.[832] Eine detaillierte Verfolgung des Nutzers kann somit trotz eines expliziten Opt-Outs erfolgen. Facebook gab dies bis 2015 auch selbst in seiner Cookie-Richtlinie an, in der es hieß:

> *Wir verwenden auch weiterhin Cookies, wenn du kein Konto besitzt oder wenn du dich von deinem Konto abgemeldet hast. Wenn du dich beispielsweise von deinem Konto abgemeldet hast, verwenden wir Cookies, um Folgendes zu unterstützen: […]*
>
> - *Bereitstellen, Auswählen, Bewerten, Messen und Verstehen der Werbeanzeigen, die wir auf und außerhalb von Facebook bereitstellen (dies beinhaltet Werbeanzeigen, die durch unsere Tochtergesellschaften oder in deren Namen bereitgestellt werden) […]*
> - *Statistiken über die Personen erstellen, die mit unseren Diensten und den Webseiten unserer Werbetreibenden und Partner interagieren*[833]

Angesichts der Tatsache, dass die Nutzer hierauf nur an so versteckter Stelle hingewiesen wurden und die Formulierung sehr unbestimmt ist, kann davon ausgegangen werden, dass dieses Vorgehen nicht von einer wirksamen Einwilligung gedeckt war.[834] In der überarbeiteten Version der Cookie-Richtlinie vom 26. Mai 2016 und der aktuellen Cookie-Richtlinie mit Stand vom 20. März 2017 findet sich der soben einleitend zitierte Satz nicht mehr.[835]

Facebook setzt den datr-Cookie indes nicht nur für seine registrierten und eingeloggten Nutzer. Vielmehr genügt es, die Domain facebook.com aufzurufen, damit u.a. der datr-Cookie gesetzt

---

832 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 96 ff.

833 https://www.facebook.com/help/cookies?fref=cub (zuletzt aufgerufen am 6.10.2015).

834 So auch *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 96 f.; zu den Anforderungen an eine wirksame Einwilligung noch ausführlich unten unter D.III.2.b).

835 https://www.facebook.com/policies/cookies/ (Stand 26. Mai 2016 und 20. März 2017).

wird.[836] Auch Nicht-Nutzer von Facebook, die sich nicht einloggen und auch kein eigenes Profil dort haben, erhalten beim Aufruf der Webseite den datr-Cookie, so dass ihr Surfverhalten auf Webseiten mit Social PlugIns im Folgenden durch diesen Cookie an Facebook gemeldet wird. Es genügt somit nicht, auf ein Facebook Konto zu verzichten, wenn man nicht von Facebook getrackt werden möchte. Vielmehr reicht ein einmaliger Aufruf der Domain facebook.com aus, um für Facebook identifizierbar zu werden, solange man den Cookie nicht manuell löscht. Ein solcher Aufruf geschieht beispielsweise beim Aufruf von Fanpages, welche über Suchmaschinen als Ergebnisse angezeigt und im Regelfall auch ohne ein Facebook Konto angesehen werden können.

Die Studie der KU Leuven zeigt zudem, dass es im Einzelfall sogar genügen kann, eine normale Webseite mit einem Social PlugIn aufzurufen, also keinerlei direkter Kontakt mit der Domain facebook.com erforderlich ist. Denn der datr-Cookie wird anscheinend auch dann gesetzt, wenn eine solche Webseite eine automatische Anfrage an die Domänen *pixel.com.facebook* oder *connect.facebook.com* startet.[837] Spätestens diese Weise, den Cookie zu erhalten, ist für Nutzer kaum noch zu vermeiden, zumal das Setzen des datr-Cookies dem Nutzer in keiner Weise angezeigt wird.

Die Studie verweist ferner darauf, dass der datr-Cookie ironischerweise selbst dann gesetzt wird, wenn man die Opt-Out-Webseite *www.youronlinechoices.eu* der European Interactive Digital Advertising Alliances besucht und auf dieser explizit angibt, dass man *nicht* von Facebook und mit diesem kooperierenden Unternehmen getrackt werden möchte.[838] In Versuchen konnte nachgewiesen werden, dass unmittelbar im Anschluss an das vermeintlich erfolgreiche Opt-Out der datr-Cookie gesetzt wurde.[839] Effektiv hat Facebook mithin über einen langen Zeitraum auch gerade die Nutzer mit dem identifizierenden datr-Cookie versehen können, die sich dem explizit entziehen wollten.

---

836 *Karg/Thomsen*, DuD 2012, 729 (730 f.); *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 82, 173 ff.; *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 97; Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 18 f.; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 6 ff.; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 7.

837 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 97 f.

838 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 98 f.; vgl. auch Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 18 f.

839 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 98 f.

Dass Facebook grundsätzlich den datr-Cookie auch auf Endgeräten von Nicht-Nutzern platziert, wenn sie nur einmal die Webseite *facebook.com* aufrufen, ohne sich anzumelden, war bereits im Audit-Report des irischen Datenschutzbeauftragten vermerkt.[840] Das Audit stellt ebenfalls fest, dass das Vorhandensein des datr-Cookies dazu führt, dass beim Aufruf einer Webseite mit Social PlugIn eine Identifikation durch Facebook möglich ist.[841] Erstaunlicherweise wurde dies aber nicht als ein Problem erachtet, sondern vielmehr lapidar mit Hinweis auf die Sicherheit Facebooks akzeptiert. Der Bericht des irischen Datenschutzbeauftragten stellt insoweit wörtlich fest:

> *„When a non-user visits www.facebook.com, three cookies are set by Facebook. Two are session cookies and one is a cookie set for two years for security reasons as outlined elsewhere. If this non-user does not clear their cookies and visits a website with a social-plugin, four cookies will be set by Facebook when delivering the plug-in to their browser.“*[842]

Zur näheren Definition des hier implizierten datr-Cookies wird auf den Anhang des Auditberichts verwiesen, wo es sodann heißt:

> *„The purpose of the datr cookie is to identify the web browser being used to connect to Facebook independent of the logged in user. This cookie plays a key role in Facebook's security and site integrity features.“*[843]

Es ist dem Auditbericht dann jedoch in keiner Weise zu entnehmen, inwiefern es für Facebooks Sicherheit erforderlich sein soll, für Nicht-Nutzer einen 2 Jahre lang gültigen Cookie zu setzen, der Aufschluss über das Nutzerverhalten auf anderen Webseiten mit Social PlugIns gibt.[844] Eine kritische Auseinandersetzung mit dem Eingriff in die nicht zuletzt aus Art. 7 und 8 GRCh

---

840 *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S.174.

841 *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 82, 176.

842 *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 82.

843 *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 176.

844 Facebook selbst informiert hierüber sehr pauschal in seinen Bestimmungen zur Verwendung von Cookies: „Die Verwendung von Cookies hilft uns dabei, die Sicherheit deines Kontos, deiner Daten sowie der Facebook-Dienste zu gewährleisten. Beispiel: Mithilfe von Cookies können wir zusätzliche Sicherheitsmaßnahmen ermitteln und einsetzen, wenn jemand versucht, ohne Berechtigung auf ein Facebook-Konto zuzugreifen; beispielsweise durch schnelles Erraten verschiedener Passwörter. […] Außerdem verwenden wir Cookies zur Bekämpfung von Aktivitäten, die gegen unsere Richtlinien verstoßen bzw. auf sonstige Art und Weise unsere Fähigkeit schwächen, die Facebook-Dienste bereitzustellen. Beispiel: Cookies helfen uns Spam und Phishing-Angriffe zu bekämpfen, indem sie es uns ermöglichen Computer zu identifizieren, die eingesetzt werden, um eine große Mengen an gefälschten Facebook-Konten zu erstellen. Mithilfe von Cookies können wir außerdem Computer ermitteln, die von Malware befallen sind und Maßnahmen ergreifen, damit diese keinen weiteren Schaden anrichten können. Darüber hinaus unterstützen Cookies uns dabei zu verhindern, dass Minderjährige sich für Facebook-Konten registrieren.“, https://www.facebook.com/policies/cookies/ (Stand 20. März 2017). Laut Angaben Facebooks im Audit des irischen Datenschutzbeauftragten soll es täglich zu bis zu 600.000 Versuchen gekommen sein, individuellen Accounts zu hacken, *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 75 f., 106.

folgenden Rechten auf Privatheit und Datenschutz, die das Setzen dieses Cookies für den Nicht-Nutzer zweifellos bedeutet, lässt sich ebenfalls nicht finden. Angesichts der Tatsache, dass das heimliche Setzen des datr-Cookies und erst Recht die resultierende Datenverarbeitung wohl kaum datenschutzrechtlich zu rechtfertigen sind, befremdet diese fehlende Auseinandersetzung sehr.[845] Im Übrigen stellt der Auditbericht in Bezug auf Facebooks Umgang mit Cookies lediglich fest:

> „FB-I makes innovative use of these cookies to identify unusual or suspicious activity on an account. The use of this information to detect, identify and prevent malicious activity on user accounts was demonstrated via sessions with the security, risk & platform operations and user operations teams. This Office is satisfied that FB-I is very pro-active in this area. In fact the only issue that has arisen is that thus far perhaps from a data collection and usage perspective it has adopted an over-zealous approach.“[846]

Der datr-Cookie ist keinesfalls für die gewünschte Nichterbringung der Facebook-Dienstleistungen für Nichtnutzer zwingend notwendig; seine Setzung und zweijährige Speicherung ist somit übereifrig („over-zealous“) im wahrsten Sinne des Wortes. Daher wäre – eine unmittelbare Anwendbarkeit vorausgesetzt – gemäß Art. 5 Abs. 3 EK-DSRL eine Einwilligung für das Setzen erforderlich.[847] Jedenfalls müsste nach § 15 Abs. 3 TMG ein Widerspruchsrecht für Nutzer eingeräumt werden, auf das diese zudem hingewiesen werden

---

845 Tatsächlich äußert auch der irische Datenschutzbeauftragte selbst Zweifel an der Rechtmäßigkeit dieser langen Speicherdauer, verweist dann aber lediglich auf eine intern mit der *Facebook Ireland Ltd.* abgeschlossene Vereinbarung, hier Abhilfe zu schaffen, deren Details aber aus Sicherheitsgründen nicht in dem Auditbericht veröffentlicht werden dürften, *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 75 f. Inwiefern eine solche Vereinbarung umgesetzt wurde, ist derzeit nicht ersichtlich.

846 *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 108.

847 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 98; Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 20; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 23; *Ernst*, NJOZ 2010, 1917 (1919); vgl. auch *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1, Rn. 48; *Martini/Fritzsche*, VerwArch (104) 2013, 449 (457); *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 92 f.; nach Ablauf der Umsetzungsfrist soll Art. 5 Abs. 3 EK-DSRL nach Auffassung einiger Datenschutzbehörden nun unmittelbar anwendbar sein, da § 15 Abs. 3 TMG nur eine Opt-Out Regelung, nicht aber die vorgeschriebene Opt-In Regelung erfordert, vgl. ULD, a.a.O.; gegen eine horizontale mittelbare Drittwirkung allerdings AK I „Staatsrecht und Verwaltung“, Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 20 f., 25; jedenfalls kritisch unter Verweis auf eine mangelnde Bestimmtheit des Art. 5 Abs. 3 EK-DSRL: *Spindler/Nink*, in: Spindler/Schuster, § 13 Rn. 6. Soweit man – entgegen der in dieser Arbeit vertretenen Auffassung – ausschließlich irisches nationales Datenschutzrecht auf Facebook für anwendbar erachtet, müsste sich dieses ebenfalls an den Voraussetzungen von Art. 5 Abs. 3 EK-DSRL messen lassen und somit zumindest ein Widerspruchsrecht, wenn nicht gar ein Opt-In Prinzip enthalten.

müssten. Dies ist aktuell bei Facebook nicht der Fall.[848] Da insbesondere Nicht-Nutzern nicht bekannt ist, dass ein solcher Cookie gesetzt und für 2 Jahre gespeichert wird, liegt auch keine Einwilligung vor, insbesondere nicht in der informierten Form, wie sie von § 4a BDSG gefordert wird. Das Setzen des datr-Cookies ist daher bei Nicht-Nutzern Facebooks in jedem Fall rechtswidrig, während es bei den registrierten Nutzern davon abhängt, ob man die die hier vertretene Auffassung teilt, dass die mit Annahme der Cookie-Richtlinie erklärte Einwilligung unwirksam ist.[849] Zu diesem Schluss kam am 9. November 2015 auch ein belgisches Gericht, das sich auf Antrag der belgischen Datenschutzbehörde mit dem datr-Cookie befasste und Facebook unter Androhung einer Geldstrafe von 250.000 € pro Tag untersagte, die Daten von Nichtnutzern zu sammeln.[850] Da die DS-GVO die durch die EK-DSRL geregelten Bereiche gemäß Art. 95 DS-GVO unberührt lässt, spricht viel dafür, dass auch nach Ablauf der Übergangsfrist die Regelung des § 15 Abs. 3 TMG in Bezug auf die Verwendung von Cookies anwendbar bleibt.

ii) Nichtbeachtung des Widerspruchsrechts und Verstoß gegen das Trennungsgebot aus § 15 Abs. 3 TMG

Die Erstellung der Statistik Facebook Insights und die hierdurch indizierten Datenverarbeitungsvorgänge sind mit den Regelungen der §§ 15 Abs. 3 u. 13 Abs. 4 Nr. 6 TMG nicht vereinbar. Mangels einer Erforderlichkeit für die Vertragsdurchführung mit den Nutzern sozialer Netzwerke kommt nach der DS-GVO allenfalls eine Erlaubnis gemäß der Interessenabwägung nach Art. 6 Abs. 1 lit. f) in Frage. In Anlehnung an die bisherige

---

848 Seit September 2015 verweist Facebook zwar immerhin durch ein eingeblendetes Banner darauf, dass Cookies im Rahmen der Verwendung der Seite gesetzt werden und dem durch eine fortgesetzte Nutzung zugestimmt wird. Ein solches Banner erfüllt nach herrschender Ansicht die notwendigen Voraussetzungen für die Aufklärung, vgl. *Schreibbauer*, in: Auernhammer, § 13 TMG Rn. 20; *Spindler/Nink*, in: Spindler/Schuster, § 11 TMG, Rn. 21. Da allerdings immer noch nicht hinreichend deutlich auf den datr-Cookie hingewiesen wird, der bereits mit dem Aufruf der Domäne facebook.com gesetzt wird und bis zu 2 Jahre gültig bleibt – auch wenn eine weitere Nutzung der Seite unterbleibt – ist dies immer noch als rechtswidrig zu betrachten. Vgl. auch *Schröder/Hawxwell*, Verletzung datenschutzrechtlicher Bestimmungen, in: Wissenschaftlicher Dienst des BT, S. 14; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 23.

849 So auch *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 98; Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 19 ff.; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 23 f.; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 24 f.; *Ernst*, NJOZ 2010, 1917 (1918 f.); zu Problemen der Einwilligung in sozialen Netzwerken auch noch ausführlich unten unter D.III.2.

850 ZD-Aktuell 2015, 04886; http://www.heise.de/newsticker/meldung/Belgisches-Gericht-Facebook-darf-keine-Daten-von-Nicht-Mitgliedern-sammeln-2912586.html. Das Urteil wurde indes in der Berufungsinstanz im Juni 2016 aufgehoben, da nach der Auffassung des Berufungsgerichts aufgrund der europäischen Hauptniederlassung Facebooks in Irland keine Zuständigkeit der belgischen, sondern nur der irischen Datenschutzbehörden begründet sei, beck-aktuell Nachrichten v. 1.7.2016.

Rechtslage und die hieraus ableitbaren Fallgruppen ist hierbei standardmäßig von einem Überwiegen der Betroffeneninteressen auszugehen, so dass die Datenverarbeitung ebenfalls unzulässig ist.[851]

Facebook ist ein Diensteanbieter im Sinne von § 2 Nr. 1 TMG. Nutzungsprofile zu Zwecken der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Telemedien-Angebots dürfen daher gemäß § 15 Abs. 3 TMG nur unter der Verwendung von Pseudonymen erstellt werden, die nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden dürfen. Zudem ist der Nutzer auf ein Widerspruchsrecht hinzuweisen, mit dem diese Form der Profilerstellung gänzlich unterbunden werden kann.[852] Dies wird auch zukünftig gemäß Art. 21 DS-GVO gelten. Aktuell hält Facebook keine dieser beiden Voraussetzungen ein. Die Nutzer werden nicht über ihr Widerspruchsrecht informiert und es ist auch keine Möglichkeit bekannt, wie dieses Widerspruchsrecht wirksam umgesetzt werden könnte, falls ein Nutzer proaktiv widerspricht.[853] Vielmehr erfolgt die zugrundeliegende Analyse und Auswertung automatisch ohne die Möglichkeit für Nutzer, sich diesen zu entziehen. Facebook behält sich in seinen Datenrichtlinien ausdrücklich vor, sämtliche zur Verfügung stehenden Informationen zu nutzen, um seine „Werbe- und Messungssysteme zu verbessern".[854] Soweit den Nutzern eine Möglichkeit zugestanden wird, die Verwendung ihrer Daten zu Werbezwecken zu „kontrollieren", ist diese innerhalb von Facebook darauf beschränkt, die „Werbeanzeigen-Einstellungen" und damit die Sichtbarkeit des eigenen Profils und eigener Handlungen für

851 Vgl. *Keppeler*, MMR 2015, 799 (782).

852 Gemäß Art. 5 Abs. 3 EK-DSRL genügt eine solche Opt-Out Regelung insbesondere bei der Profilerstellung unter Einsatz von Cookies nicht. Vielmehr wird in der Richtlinie ausdrücklich eine Opt-In Lösung gefordert. Auf die Frage, ob angesichts der bereits abgelaufenen Umsetzungsfrist Art. 5 Abs. 3 EK-DSRL nun direkt anwendbar ist, mit der Folge, dass § 15 Abs. 3 TMG insoweit zurücktritt und bloße Opt-Out Regelungen rechtswidrig sind, soll hier indes nicht näher eingegangen werden, da hier bereits die Bedingungen der Opt-Out Regelung nicht erfüllt werden.

853 ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 23; *Schröder/Hawxwell*, Verletzung datenschutzrechtlicher Bestimmungen, in: Wissenschaftlicher Dienst des BT, S. 14.

854 „Wir sammeln die Inhalte und sonstigen Informationen, die du bereitstellst, wenn du unsere Dienste nutzt; dazu gehören auch deine Registrierung für ein Konto, das Erstellen oder Teilen von Inhalten sowie das Versenden von Nachrichten bzw. das Kommunizieren mit anderen. […] Wir nutzen die uns zur Verfügung stehenden Informationen, um unsere Werbe- und Messungssysteme zu verbessern, damit wir dir auf unseren Diensten und außerhalb dieser relevante Werbeanzeigen anzeigen und die Wirksamkeit und Reichweite von Werbeanzeigen und Diensten messen können.", https://www.facebook.com/privacy/explanation (Stand 29. September 2016).

Dritte einzuschränken.[855] Dies erfüllt nicht die Voraussetzungen eines Widerspruchsrechts im Sinne von § 15 Abs. 3 TMG bzw. Art. 21 DS-GVO.[856]

Zudem liegt ein offensichtlicher Verstoß gegen das Trennungsgebot aus §§ 15 Abs. 3, 13 Abs. 4 Nr. 6 TMG vor. Die für die Erstellung von Insights verwendeten personenbezogenen Daten wie Alter, Nationalität und Interessen lassen sich den bei dem Besuch der Fanpage anfallenden Bestands- und Nutzungsdaten nicht entnehmen. Sie werden von Facebook folglich aus anderen Datenbeständen ermittelt. Hierbei wird es sich schwerpunktmäßig um die gespeicherten Nutzerprofile handeln. Diese sind aufgrund des in den Nutzungsbedingungen vorgeschriebenen Klarnamenszwangs indes zwingend mit dem Klarnamen der Person verbunden. Selbst wenn Facebook keinen Zugriff auf den Klarnamen hat, handelt es sich bei den demografischen, geografischen oder interessengebundenen Ergänzungen um personenbezogene Daten, wenn die Person für Facebook identifizierbar ist, wovon aufgrund der ebenfalls gespeicherten BrowserIDs, IP-Adressen und sonstigen vergleichbaren Daten auszugehen ist.[857] In jedem Fall werden somit entgegen § 15 Abs. 3 TMG die pseudonymen Nutzungsprofile mit Daten über den Träger des Pseudonyms zusammengeführt, was einen Datenschutzverstoß begründet.[858] Diese Wertung ist auf die Interessenabwägung des Art. 6 Abs. 1 lit. f) DS-GVO zu übertragen, so dass in aller Regel auch nach der DS-GVO keine legitime Datenverarbeitung vorliegen würde.

iii) Missachtung der Aufklärungspflichten aus § 13 Abs. 1 TMG bzw. Art. 12 ff. DS-GVO

Facebook verstößt zudem gegen seine Aufklärungspflichten aus § 13 Abs. 1 TMG bzw. Art. 12 ff. DS-GVO. Zwar präsentiert Facebook mittlerweile eine sehr umfangreiche „Datenrichtlinie", in welcher es darüber zu informieren versucht, welche Daten es sammelt, wie und zu welchen Zwecken es diese verarbeitet und an welche Dritten es diese weitergibt.[859] Allerdings ist diese Richtlinie immer noch von zahlreichen Unklarheiten und großer Vagheit geprägt. Einige Beispiele hierfür sind:

---

855 https://www.facebook.com/about/ads/#568137493302217.

856 *Weichert*, JBÖS 2012/2013, 379 (380); *Karg/Thomsen*, DuD 2012, 729; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 23; instruktiv: *Hullen/Roggenkamp*, in: Plath, § 15 TMG, Rn. 10 f., 30; *Spindler/Nink*, in: Spindler/Schuster, § 15 TMG, Rn. 9 ff.

857 Zur Personenbeziehbarkeit bereits oben unter C.III.4.c).

858 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (2); *Karg/Thomsen*, DuD 2012, 729 (735 f.); ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 23 f.; vgl. auch *Spindler/Nink*, in: Spindler/Schuster, § 15 TMG, Rn. 9.

859 https://www.facebook.com/privacy/explanation (Stand 29. September 2016).

> *„Wir erhalten von Drittpartnern Informationen über dich und deine Aktivitäten auf und außerhalb von Facebook; beispielsweise von einem Partner, wenn wir gemeinsam Dienste anbieten, oder von einem Werbetreibenden über deine Erfahrungen oder Interaktionen mit ihm."*
>
> *„Wir erhalten Informationen über dich von Unternehmen, die sich im Besitz von Facebook befinden oder von diesem betrieben werden, im Einklang mit deren Bedingungen und Richtlinien."*
>
> *„Sollten sich die Eigentums- oder Machtverhältnisse aller bzw. eines Teils unserer Dienste oder ihrer Vermögenswerte ändern, können wir deine Informationen an den neuen Eigentümer übertragen."*
>
> *„Wir übertragen Informationen an Anbieter, Dienstleister und sonstige Partner, die unser Unternehmen weltweit unterstützen, beispielsweise indem sie Dienstleistungen für eine technische Infrastruktur zur Verfügung stellen, analysieren, wie unsere Dienste genutzt werden, die Wirksamkeit von Werbeanzeigen und Diensten messen, eine Kundenbetreuung anbieten, Zahlungen ermöglichen oder wissenschaftliche Studien und Umfragen durchführen. Diese Partner müssen im Einklang mit dieser Datenrichtlinie und den mit ihnen geschlossenen Vereinbarungen strenge Geheimhaltungspflichten einhalten."*[860]

Die Aufklärung kommt hier eher einer Blanko-Erklärung gleich. Weder ist für Nutzer völlig einschätzbar, welche Informationen und Daten konkret über sie erhoben werden, noch an wen sie für welche konkreten Zwecke weitergegeben werden. Eine bloße Blanko-Erklärung erfüllt aber nicht die Voraussetzungen einer bewussten und eindeutigen Einwilligung im Sinne von § 13 Abs. 2 Nr. 1 TMG bzw. einer freiwilligen und informierten Einwilligung im Sinne von § 4a BDSG.[861] Auf eben diesen Maßstab muss es aber ankommen um zu beurteilen, ob die Aufklärung hinreichend ist, da sie ansonsten leerläuft.[862] Es handelt sich somit weder um eine angemessene Unterrichtung nach § 13 Abs. 1 TMG noch sind die Voraussetzungen einer Einwilligung nach § 12 Abs. 1 TMG erfüllt.[863] Dies gilt auch für eine Einwilligung nach Art. 7 DS-GVO i.V.m. den Erwägungsgründen 32 und 42 DS-GVO.

iv) Rechtswidrige Statuierung eines Klarnamenzwangs

Zuletzt verletzt Facebook mit dem in den Nutzungsbedingungen unter Punkt 4 statuierten Klarnamenzwang[864] jedenfalls nach bisheriger Rechtslage das in § 13 Abs. 6 TMG garantierte

---

860 https://www.facebook.com/privacy/explanation (Stand 29. September 2016).

861 *Weichert*, JBÖS 2012/2013, 379 (380); *Karg/Thomsen*, DuD 2012, 729 (735); ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 21; *Simitis*, in: Simitis, BDSG, § 4a Rn. 77 m. zahlreichen w.N.; hierzu noch unten ausführlich unter D.III.2.b).

862 Vgl. *Piltz*, Soziale Netzwerke, S. 117; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 21 f.

863 *Martini/Fritzsche*, VerwArch (104) 2013, 449 (458 f.); *Schröder/Hawxwell*, Verletzung datenschutzrechtlicher Bestimmungen, in: Wissenschaftlicher Dienst des BT, S. 15; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 20 ff.

864 https://www.facebook.com/legal/terms?ref=pf (Stand 30. Januar 2015).

Recht der anonymen bzw. jedenfalls pseudonymen Telemediennutzung. Dieses Recht steht zwar in einem Spannungsverhältnis zu Belangen der Sicherheit und der allgemeinen Rechtsdurchsetzung bei Rechtsverstößen in sozialen Netzwerken. Jedenfalls der Zwang, sich anderen Nutzern gegenüber mit seinem richtigen Namen auszuweisen, stellt aber einen Verstoß gegen § 13 Abs. 6 TMG dar.[865] Inwieweit § 13 Abs. 6 TMG in einem Konflikt zur möglichen Impressumspflicht besteht und wie dieser gegebenenfalls aufzulösen ist, wird ebenso wie das Spannungsverhältnis zu Belangen der Sicherheit und Rechtsdurchsetzung ausführlich unten unter D.II.2 diskutiert.

Zugunsten von Fanpage-Betreibern sei aber angemerkt, dass sie von diesem spezifischem Datenschutzverstoß Facebooks in Bezug auf die Erstellung von Facebook Insights nicht maßgeblich profitieren. Wie bereits dargelegt wurde, stammen viele der für Facebook Insights verwendeten Informationen aus allgemeinen Profildaten, über Cookies und Social PlugIns gesammelte Daten und Big Data Analysen. Facebook gibt – nach eigenen Angaben – den Klarnamen auch nicht an die Fanpage-Betreiber weiter, sondern nur anonymisierte Nutzerprofile.[866]

Obwohl in dem Klarnamenzwang gegenüber Nutzern ein klarer Datenschutzverstoß liegt, fehlt es daher mangels eines Profitierens der Fanpage-Betreiber an einem hinreichenden Zurechnungszusammenhang. Auch deshalb soll auf die hiermit verbundenen Probleme an dieser Stelle noch nicht vertieft eingegangen werden, sondern es nach unten verwiesen werden. Dies gilt umso mehr, als die DS-GVO – ebenso wie die DSRL – kein vergleichbares Recht enthalten, so dass es fraglich ist, inwieweit dieses Recht nach Ablauf der Übergangsfrist überhaupt noch anwendbar sein wird.

v) Zwischenergebnis

Die soeben exemplarisch dargelegten Datenschutzverstöße zeigen, dass es erhebliche Pflichtverletzungen durch Facebook gibt und auch mit Anwendbarkeit der DS-GVO geben wird. Diese betreffen auch die bei der Nutzung von Fanpages anfallenden Daten. In erster Linie ist für diese Datenschutzverstöße natürlich Facebook selbst datenschutzrechtlich verantwortlich, da es die Kontrolle über Zwecke und Mittel der Datenverarbeitung innehat und

865 *Buchner*, Facebook zwischen BDSG und UWG, in: FS Köhler, S. 55; *Weichert*, JBÖS 2012/2013, 379 (380); *Caspar*, ZD 2015, 12 (14); hierzu noch ausführlich unten unter D.II.2.

866 https://www.facebook.com/privacy/explanation# (Stand 29. September 2016).

den wirtschaftlichen Nutzen aus den erhobenen und verarbeiteten Daten zieht.[867] Auch die Statistik Facebook Insights beruht indes maßgeblich auf einigen dieser Datenschutzverstöße. Jedenfalls mittelbar profitieren daher auch die Fanpage-Betreiber. Im Folgenden soll daher untersucht werden, inwieweit hieraus eine, gegebenenfalls mittelbare, datenschutzrechtliche Verantwortlichkeit der Fanpage-Betreiber erwachsen kann.

bb) Unmittelbare datenschutzrechtliche Verantwortlichkeit der Fanpage-Betreiber

In Ermangelung eines eigenen Verantwortlichkeitsbegriffs in den §§ 11 ff. TMG ist gemäß § 12 Abs. 3 TMG auf den Begriff der verantwortlichen Stelle nach § 3 Abs. 7 BDSG zurückzugreifen.[868] Inwieweit Fanpage-Betreiber hiernach für den Umgang mit Bestands- und Nutzungsdaten (mit-)verantwortlich sind – oder ob neben § 3 Abs. 7 BDSG noch anderweitig eine Verantwortlichkeit für diesen Umgang begründet werden kann –, ist stark umstritten.[869] Zur Klärung ist eine Klage bei dem Bundesverwaltungsgericht anhängig, welches mit Beschluss vom 25.02.2016 unter anderem diese Frage mit Blick auf die Auslegung der zugrunde liegenden Regelung des Art. 2 lit. d) DSRL dem EuGH zur Vorabentscheidung vorgelegt hat.[870] Kern des Problems ist, ob die Initiierung und Veranlassung der Datenübertragung an den Anbieter des sozialen Netzwerks durch das Betreiben der Fanpage einen hinreichenden Einfluss auf die Zwecke und Mittel der Datenverarbeitung begründet.

---

867 Vgl. auch *Karg/Thomsen*, DuD 2012, 729 (733); Exakt welche Stelle von Facebook die Entscheidungsbefugnis über die Zwecke und Mittel dieser Datenverarbeitung hat – ob dies *Facebook Inc.*, *Facebook Ireland Ltd.* oder die *Facebook Germany GmbH* ist – kann hier dahinstehen, da wie oben unter C.II.4.b)cc) gezeigt wurde, eine jeweilige Zurechnung der Datenverarbeitung stattfindet, da diese Unternehmen in dieser Hinsicht in einem wirtschaftlich untrennbaren Kontext zusammenarbeiten.

868 *Gerhold*, ZIS 2015, 156 (160); *Moos*, in: Taeger/Gabel, § 11 TMG Rn. 28; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 16; *Piltz*, CR 2011, 657 (662).

869 Für eine Verantwortlichkeit plädieren u.a. *Weichert*, ZD 2014, 605 (606 ff.); *Düsseldorfer Kreis*, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.pdf?__blob=publicationFile&v=1, 2011, S. 2; Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 11 f.; tendenziell auch AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 18 f.; gegen eine Verantwortlichkeit stehen u.a. VG Schleswig, ZD 2014, 51 (52 ff.); OVG Schleswig, ZD 2014, 643 (643 ff.); *Maisch*, Informationelle Selbstbestimmung, S. 216; *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (124); *Voigt*, Webbrowser Fingerprints, in: Taeger (Hrsg.), LaaS, Recht im Internet und Cloudzeitalter, S. 168; *Ders./Alich*, NJW 2011, 3541 (3543); auf das Maß an Einfluss auf die Verarbeitungsmöglichkeiten abstellend und damit grundsätzlich eher verneinend *Dammann*, in: Simitis, BDSG, § 3 Rn. 224.

870 BVerwG, ZD 2016, 393 (393 ff.); Das Verfahren wird geführt zwischen der Wirtschaftsakademie Schleswig-Holstein GmbH und dem Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) als Revision zu der Entscheidung OVG Schleswig, ZD 2014, 643 ff.

Indem Art. 4 Nr. 7 DS-GVO den Verantwortlichkeitsbegriff weitgehend wortgleich zur bisherigen Rechtslage übernimmt, wird sich das Problem unverändert auch in der Zukunft stellen. Lediglich die Abgrenzung zwischen TMG und BDSG wird gegebenenfalls entfallen.

Die Betreiber von Fanpages setzen, wie bereits dargelegt, einen Anlass dafür, dass durch den Besuch ihrer Fanpage Bestands- und Nutzungsdaten an Facebook übermittelt werden.[871] Sie übermitteln oder speichern diese aber nicht selbst. Vielmehr liegt ein technischer Automatismus vor, der beim Aufruf der Seite dazu führt, dass diese Daten direkt an Facebook gesendet werden. Weder erfolgt eine Zwischenspeicherung beim Betreiber der Fanpage, noch gehen sie überhaupt durch seine Hände.[872] Entsprechend haben die Fanpage-Betreiber keinen Einfluss darauf, wie und zu welchen Zwecken diese Daten gespeichert und verwendet werden. Sie erhalten von Facebook lediglich einen ausführlichen, aber anonymen statistischen Überblick über die Besucher ihrer Fanpage in Form des Werkzeugs „Facebook Insights". Diese ist unter anderem nach Alter und Geschlecht aufgeschlüsselt und ermöglicht den Fanpage-Betreibern, ihr Angebot besser auf ihre Zielgruppe abzustimmen.[873] Als anonymisierte Daten sind diese indes nicht personenbezogen und fallen daher auch nicht unter die datenschutzrechtlichen Regelungen des BDSG oder TMG.

Befürworter einer unmittelbaren datenschutzrechtlichen Verantwortlichkeit von Fanpage-Betreibern verweisen darauf, dass diese zwar keine Kontrolle hinsichtlich des „Wie" der Datenverarbeitung durch Facebook haben, sehr wohl aber über das „Ob" entscheiden können.[874] Anstelle einer Fanpage könnten sie auch eine klassische eigene Webseite betreiben, auf der sie selbst die entsprechenden Bestands- und Nutzungsdaten erheben würden, anstatt diesen Vorgang an Facebook auszulagern. Indem sie sich für den Betrieb einer Fanpage bei Facebook entschieden, träfen sie die maßgebliche Entscheidung zum „Ob" der Datenverarbeitung. Würden sie den Betrieb der Fanpage unterlassen und auf Alternativen zugreifen, hätte Facebook auch keine Möglichkeit, die Daten zu erheben. Im Verhältnis zur

---

871 *Karg/Thomsen*, DuD 2012, 729 (733); *Weichert*, ZD 2014, 605 (607 f.); *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (3); Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 11 f.

872 *Gerhold*, ZIS 2015, 146 (160); *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG, Rn. 11; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 11, 16; *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (123); *Voigt/Alich*, NJW 2011, 3541 (3542).

873 *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 11; *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (123).

874 *Weichert*, ZD 2014, 605 (608); *Karg/Thomsen*, DuD 2012, 729 (733); ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S.17, 22 f.; Bayrischer Landesdatenschutzbeauftragter, https://www.datenschutz-bayern.de/technik/orient/oh_fanpages.pdf, S. 12; vgl. auch Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 13 f.; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 17 f.

Entscheidung über das konkrete „Wie“ der Datenverarbeitung sei dies der entscheidende Schritt, so dass die Fanpage-Betreiber als Verantwortliche zu sehen seien.[875] Ergänzend wird vertreten, dass es sich bei dem Vertrag über den Betrieb der Fanpage um eine Form der Auftragsdatenverarbeitung handele, bei der der Fanpage-Betreiber als Auftraggeber gemäß § 11 BDSG verantwortlich sei.[876]

Dieser Ansicht ist nicht zu folgen. Selbst nach dem in dieser Arbeit vertretenen weiten wirtschaftlich-funktionellen Verantwortlichkeitsbegriff ist die Entscheidungskompetenz des Fanpage-Betreibers über das „Ob“ nicht hinreichend, um eine unmittelbare Verantwortlichkeit zu begründen. Die Annahme einer Auftragsdatenverarbeitung verfehlt zudem die Realität der Vertragsbeziehung zwischen dem Fanpagebetreiber und Facebook, in welcher ersterem keinerlei Weisungsrecht und Kontrollbefugnisse zukommen.[877]

Zwar kommt es in der gebotenen europarechtskonformen weiten Auslegung des Begriffs der verantwortlichen Stelle weniger darauf an, ob ein Verantwortlicher tatsächlich selbst Schritte der Datenverarbeitung ausführt. Es spricht daher nicht prinzipiell gegen eine Verantwortlichkeit der Fanpage-Betreiber, dass die konkrete Datenverarbeitung von Facebook durchgeführt wird. Die bloße Entscheidung über das „Ob“ der Datenverarbeitung in Form der Entscheidung über die Gründung der Fanpage kann aber nicht als hinreichende Entscheidungsbefugnis über Zwecke und Mittel der Datenverarbeitung angesehen werden, wie dies gemäß Art. 2 lit. d) DSRL oder zukünftig Art. 4 Nr. 7 DS-GVO erforderlich wäre.[878] Würde eine hinreichende Entscheidungsbefugnis bereits bejaht, wenn nur über die Initiierung einer Datenverarbeitung entschieden werden kann, würde die differenzierte Frage nach dem konkreten Zweck und erst Recht nach den eingesetzten Mitteln obsolet. Es entstünde eine gleichsam gesamtschuldnerische Haftung, bei der nicht derjenige zur Verantwortung gezogen wird, der tatsächlich Einfluss auf die Form der Datenverarbeitung nehmen kann, sondern jeder, der diese initiiert bzw. teilweise auch nur schlicht in Kauf nimmt. Im Zeitalter ubiquitärer Datenverarbeitung würde dies eine faktische Aufhebung differenzierter

875 *Weichert*, ZD 2014, 605 (608); ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S.17 f.; Konferenz der Datenschutzbeauftragten, https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf, S. 11 f.

876 ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 17 f.

877 OVG Schleswig, ZD 2014, 643 (644); VG Schleswig, ZD 2014, 51 (53); *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (6); *Gerhold* , ZIS 2015, 156 (160); *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG, Rn. 11; *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (123); vgl. auch *Schröder/Hawxwell*, Verletzung datenschutzrechtlicher Bestimmungen, in: Wissenschaftlicher Dienst des BT, S. 8 f.

878 So auch *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (6 f.); vgl. zudem *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG, Rn. 11; *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (124).

Verantwortungszuweisung bedeuten und quasi eine abstrakte „Datenverarbeitungsfolgenverantwortung“ begründen. Dies mag zwar eine denkbare Lösung für den Umgang mit den Problemen vernetzter Datenverarbeitung darstellen. Es entspricht jedoch nicht dem vom Gesetz vorgesehenen Ansatz der konkreten Verantwortungszuweisung aufgrund eigener Handlung oder faktischer und rechtlicher Entscheidungsbefugnisse.[879]

Auch nach der weiten funktionell-wirtschaftlichen Auslegung des EuGH können Fanpage-Betreiber also nicht als unmittelbar verantwortliche Stelle angesehen werden. Der Betrieb ihres eigenen Geschäfts und der Betrieb der Fanpage sind nicht in einem Maße wirtschaftlich untrennbar miteinander verbunden wie dies bei dem Betrieb einer Suchmaschine und dem zugehörigen Werbegeschäft der Fall ist.[880] Die Fanpage generiert zwar eine höhere Reichweite des eigenen Angebots und zudem bietet die Funktion „Facebook Insights“ hilfreiche Zusatzinformationen über die erreichte Kundengruppe. Der Fanpage-Betreiber könnte aber in aller Regel ohne existentielle Konsequenzen für sein Geschäft auch auf eine andere Form des Marketings ausweichen und etwa eine private Webseite einrichten. Diese hätte zwar im Zweifel eine geringere Reichweite wäre und nicht an individuelle Nutzerinteressen angepasst. Insofern darf nicht unterschätzt werden, wie wichtig zielgerichtetes Marketing heutzutage ist, um überhaupt noch einen Effekt auf die Zielgruppe zu haben.[881] Trotzdem ist es zumindest unwahrscheinlich, dass das Social-Media-Marketing bereits eine so hohe Bedeutung erlangt hat, dass ein wirtschaftlicher Betrieb des eigenen Unternehmens nicht mehr ohne es möglich ist, insbesondere wenn etwaige Beschränkungen auch alle Konkurrenten treffen würden.[882] Es liegt somit in aller Regel kein untrennbarer Zusammenhang zwischen dem Betrieb der Fanpage und dem Betrieb des eigenen Geschäfts im Sinne des funktionell-wirtschaftlichen Verantwortlichkeitsbegriffs vor.

---

879 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (5); *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (124); Piltz, CR 2011, 657 (662).

880 Vgl. zum funktionell-wirtschaftlichen Verantwortlichkeitsbegriff und der *Google*-Entscheidung des EuGH bereits ausführlich oben unter C.II.4.b)bb).

881 *Lichtnecker*, GRUR 2013, 135 (135 f.); vgl. auch Bitkom, https://www.bitkom.org/Publikationen/2013/Studien/Soziale-Netzwerke-dritte-erweiterte-Studie/SozialeNetzwerke-2013.pdf, S. 54 ff. zur Effektivität und Akzeptanz von Werbung in sozialen Netzwerken.

882 Vgl. *Lichtnecker*, GRUR 2013, 135 (135 f.).

Fanpage-Betreiber sind auch nicht als Auftraggeber einer Auftragsdatenverarbeitung gemäß § 11 BDSG bzw. Art. 28 DS-GVO einzuordnen.[883] In einem sehr weiten, eher umgangssprachlichen Verständnis des Begriffs des Auftrags kann man zwar sagen, dass der Fanpage-Betreiber Facebook damit „beauftragt", eine Fanpage mit dem vom Betreiber selbst gewählten Inhalt zu erstellen und bereitzuhalten. Es ist unbestritten, dass der Fanpage-Betreiber insoweit die initiierende Stelle ist, die die letztendliche Entscheidung über das „Ob" des Betriebs trifft. Es trifft ferner zu, dass die Fanpage-Betreiber Facebook als einen externen Dienstleister nutzen, um ein effizientes Marketing mit hoher Reichweite und individueller Ausrichtung zu betreiben anstelle einer eigenen Webseite.[884]

Allerdings kommt den Fanpage-Betreibern abseits ihrer inhaltlichen Gestaltungsfreiheit – wie bereits festgestellt – keinerlei Weisungsbefugnis gegenüber Facebook zu.[885] Facebook stellt ihnen lediglich die Infrastruktur für die Fanpage zur Verfügung, um durch den so generierten Nutzerverkehr selbst Daten über diese Nutzer erheben und nutzen zu können. Ähnlich wie bei nutzergenerierten Inhaltsdaten ist es für Facebook im Ergebnis gleichgültig, mit welchen Absichten und zu welchen Zwecken eine Fanpage betrieben wird. Das Geschäftsmodell von Facebook erfordert schlicht, so viele Daten wie möglich über seine Nutzer und darüber hinaus auch anderen Internetnutzern zu erheben, diese in Profilen zu verarbeiten und hieraus Gewinne zu erwirtschaften. Fanpages eignen sich hierfür besonders gut, da sie eine eher unbewusste Datenpreisgabe der Nutzer provozieren. So werden beispielsweise Interessen beiläufig dadurch bekundet, auf welchen Seiten der Nutzer wie lange verbleibt bzw. welche Seiten er „liked".[886] Eine weitergehende Verarbeitung der Bestands- und Nutzungsdaten, die beim Besuch der Nutzer auf einer Fanpage anfallen, ist für Facebook somit von erheblicher Bedeutung.

Dieses Geschäftsmodell unterscheidet Facebook von beispielsweise Cloud-Dienstleistern, deren Tätigkeit gemeinhin als Anwendungsfall der Auftragsdatenverarbeitung behandelt wird, obwohl auch bei diesen dem Auftraggeber zumindest faktisch kaum eine Weisungsbefugnis zukommt, die den Anforderungen von § 11 Abs. 2 BDSG bzw. Art. 28 Abs. 3 DS-GVO

---

883 So auch *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (5 f.); *Gerhold* , ZIS 2015, 156 (160); *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG, Rn. 11; *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 89; *Martini/Fritzsche*, VerwArch (104) 2013, 449 (462 f.); a.A.: ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 17 f.

884 ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 17 f.; vgl. auch *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (2 f.).

885 OVG Schleswig, ZD 2014, 643 (644); VG Schleswig, ZD 2014, 51 (53); *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (6); *Gerhold* , ZIS 2015, 156 (160); *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG, Rn. 11; *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (124); *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 89 f.; AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 16 f.

886 Hierzu bereits oben unter B.II.2.b).

entspricht.[887] Ein Cloudanbieter stellt Speicherplatz für den Auftraggeber zur Verfügung und ermöglicht den Zugriff im vereinbarten Rahmen. Er ist ebenso wie Facebook wirtschaftlich darauf angewiesen, dass sein Angebot angenommen wird, der Speicher also gebraucht wird. Soweit er die gespeicherten Daten unabhängig von konkreten Weisungen des Auftraggebers speichert und verwendet, wird dies aber in aller Regel mit Effizienzgewinnen und allgemeinen Geschäftsstrukturen zu begründen sein. Er verfolgt mit der unabhängigen Datenverarbeitung keine eigenen Zwecke. Für Facebook stellt es dagegen gerade das Geschäftsmodell dar, die über die Fanpage erhobenen Daten weiterzuverarbeiten, ohne die hieraus gewonnenen Informationen publik zu machen, da sie ansonsten wertlos würden. Es ist somit schon im Grundprinzip des derzeitigen Fanpage-Betriebs enthalten, dass Facebook außerhalb der Kontrolle des Fanpage-Betreibers mit den Daten umgeht. Eine Weisungsbefugnis und Kontrollmöglichkeit des Fanpage-Betreibers zu bejahen, würde somit nicht nur faktisch eine Fiktion darstellen[888], sondern darüber hinaus auch dem Sinn und Zweck des gesamten Vertragsverhältnisses widersprechen. Der Fanpage-Betreiber kann daher nicht als Auftragsgeber einer Auftragsdatenverarbeitung angesehen werden.

Eine unmittelbare Verantwortlichkeit der Fanpagebetreiber für die durch Facebook beim Besuch der Fanpage erhobenen Bestands- und Nutzungsdaten scheidet daher aus.[889] Diese Feststellung beantwortet freilich noch nicht die Frage, ob sie sich den Datenumgang Facebooks nicht dennoch in irgendeiner Form zurechnen lassen müssen. Gerade weil nicht zu bestreiten ist, dass die Betreiber zumindest den Anlass für die Datenverarbeitung durch Facebook setzen und selbst in erheblichem Maße hiervon profitieren, bestünde eine potentielle Schutzlücke, wenn sie sich jeglicher Verantwortung entziehen und ausschließlich auf Facebook verweisen könnten.[890] Für die Betroffenen gestaltet es sich nämlich im Regelfall erheblich schwieriger, einen rechtskonformen Datenumgang gegenüber einem großen Anbieter eines sozialen Netzwerks wie Facebook einzuklagen, als gegenüber einem Unternehmen vor Ort, das diese möglicherweise rechtswidrige Infrastruktur zu seinem eigenen Vorteil nutzt. Zudem mag es

---

887 Zum Auftragsverhältnis beim Cloud-Computing: Art. 29 DatSchGruppe, Stellungnahme 05/2012, WP 196, S. 9 ff.; *Petri*, in: Simitis, BDSG, § 11 Rn. 30 m.w.N.; *Wagner/Blaufuß*, BB 2012, 1751 (1752); *Pohle/Ammann*, CR 2009, 273 (276 f.).

888 OVG Schleswig, ZD 2014, 643 (644); VG Schleswig, ZD 2014, 51 (53); *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (124); AK I „Staatsrecht und Verwaltung", Ergebnisbericht Datenschutz in Sozialen Netzwerken, 2012, S. 16 f.

889 So auch OVG Schleswig, ZD 2014, 643 (644); VG Schleswig, ZD 2014, 51 (53); *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (9); *Gerhold* , ZIS 2015, 156 (160); *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG, Rn. 11; *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 92; *Dammann*, in: Simitis, BDSG, § 3 Rn. 224.

890 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (11); *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (124 f.).

einigen Nutzern nicht einmal bewusst sein, dass sie sich in einem Angebot des Betreibers des sozialen Netzwerks befinden. Sie könnten vielmehr wegen der inhaltlichen Gestaltung der Fanpage denken, dass sie direkt mit deren inhaltlichem Betreiber zu tun haben.[891] Aufgeworfen ist damit die Frage nach einer möglichen mittelbaren Verantwortlichkeit des Fanpage-Betreibers.

cc) Mittelbare Verantwortlichkeit privater Fanpage-Betreiber

Fanpage-Betreiber setzen den Anlass für die aus dem Besuch einer Fanpage resultierenden rechtswidrigen Datenverarbeitung durch Facebook und profitieren hiervon in der zuvor beschriebenen Form.[892] Immer wieder stattfindende und teilweise mit Erfolg gekrönte Verwaltungs- und Gerichtsverfahren stellen zudem für die Betreiber erkennbare Anhaltspunkte dar, dass Facebook Datenschutzregeln im Umgang mit den so erhaltenen Daten verletzt.[893] Das allgemeine Polizei- und Ordnungsrecht kennt – in Abweichung von der Theorie der unmittelbaren Verursachung – für solche Konstellationen die dogmatische Figur des Zweckveranlassers zur Begründung einer mittelbaren Verantwortlichkeit. Im Zivilrecht ist zudem die Störerhaftung als Form der mittelbaren Verantwortlichkeit im Internet anerkannt.[894] Zu überlegen ist, inwieweit diese Figuren auf die datenschutzrechtliche Verantwortlichkeit übertragen werden können. Diese Frage war in letzter Zeit vermehrt Gegenstand wissenschaftlicher Diskussionen[895] und ist nicht zuletzt Gegenstand des bereits erwähnten am Bundesverwaltungsgericht anhängigen Revisionsverfahrens und nunmehr Vorabentscheidungsverfahrens am EuGH.[896] Entscheidend hierfür ist insbesondere, inwieweit das Datenschutzrecht als abschließendes spezielles Ordnungsrecht einzustufen und somit ein Rückgriff auf das allgemeine Polizei- und Ordnungsrecht zulässig ist (hierzu i)). Für eine Lösung innerhalb des Datenschutzrechts plädieren dagegen *Martini* und *Fritzsche*, indem sie eine „Auswahlverantwortlichkeit" aus § 11 Abs. 2 S. 1 BDSG i.V.m. § 4 BDSG ableiten, die neben § 3 Abs. 7 BDSG zur Adressatenbestimmung des § 38 Abs. 5 BDSG herangezogen werden könne (hierzu ii)(1)).

---

891 *Kauß*, Revisionsbegründung zum BVerwG, Az. 1 C 28.14 vom 02.01.2015, S. 38 ff.

892 Oben unter D.I.3.c).

893 LG Berlin, ZD 2012, 276 (277 ff.); KG Berlin, ZD 2014, 412 (414 ff.); LG Berlin, ZD 2015, 133 (134 ff.); vgl. auch BVerwG, ZD 2016, 393 (393 ff.).

894 Hierzu bereits oben unter D.I.3.a)bb).

895 Die Möglichkeit einer mittelbaren Verantwortlichkeit und Störerhaftung bejahen: *Petri*, ZD 2015, 103 (104 ff.); *Kauß*, Revisionsbegründung zum BVerwG, Az. 1 C 28.14 vom 02.01.2015, S. 50 ff.; *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (124 f.); *Piltz*, CR 2011, 657 (662 f.); ablehnend: OVG Schleswig, ZD 2014, 643 (644); VG Schleswig, ZD 2014, 51 (54); *Gerhold*, ZIS 2015, 156 (160); *Piltz*, K&R 2014, 80 (85); *Voigt/Alich*, NJW 2011, 3541 (3543).

896 BVerwG, ZD 2016, 393 (393 ff.).

Zudem stellt sich die Frage nach der Antwort der DS-GVO auf dieses Problem (hierzu iii)). Zur Vermeidung von übergroßer Komplexität und unnötiger Vermischung wird diese Frage – abweichend von dem sonstigen Vorgehen in dieser Arbeit – erst im Anschluss an die Klärung der bisherigen Rechtslage beantwortet. Vorweggenommen sei an dieser Stelle, dass angesichts der weitgehend wortgleichen Übernahme des bisherigen Verantwortlichkeitsbegriffs in Art. 4 Nr. 7 DS-GVO keine befriedigende Lösung erfolgt, so dass lediglich zu klären ist, inwieweit ein Rückgriff auf ergänzende Verantwortlichkeitszuschreibungen bzw. das grundsätzliche Konzept der mittelbaren Verantwortlichkeit im Rahmen der Vorschriften der DS-GVO möglich ist. Im Ergebnis gibt es dabei nach hier vertretener Auffassung keine grundlegenden materiellen Änderungen gegenüber der bisherigen Rechtslage.

Die praktische Konsequenz einer mittelbaren Verantwortlichkeit wäre, dass datenschutzrechtliche Aufsichtsbehörden Anordnungen gemäß § 38 Abs. 5 BDSG und zukünftig unter anderem Art. 58 DS-GVO auch gegen die Betreiber von Fanpages richten könnten, nicht nur gegen Facebook selbst als die unmittelbar verantwortliche Stelle. Zudem könnten gegebenenfalls auch Unterlassungsansprüche direkt gegen den Fanpage-Betreiber geltend gemacht werden.

i) Keine abschließende Regelung durch das Datenschutzrecht

Das Datenschutzrecht stellt besonderes Ordnungsrecht mit speziellen Regelungen zur Verantwortlichkeit dar. Auf das allgemeine Ordnungsrecht und die Figur des Zweckveranlassers bzw. auf die zivilrechtliche Störerhaftung kann daher nur dann zurückgegriffen werden, wenn die Regelungen im Datenschutzrecht nicht abschließend sind. Inwieweit dies der Fall ist, ist durch Auslegung zu ermitteln.[897]

Adressat der im allgemeinen Datenschutzrecht geregelten Pflichten ist die verantwortliche Stelle gemäß § 3 Abs. 7 BDSG bzw. Art. 4 lit. d) DSRL und zukünftig Art. 4 Nr. 7 DS-GVO. Als *lex specialis* ist es als abschließend zu betrachten, soweit positive Verhaltenspflichten im Umgang mit personenbezogenen Daten aufgestellt werden. Dies ergibt sich systematisch daraus, dass andernfalls der Grundsatz der Spezialität zu einfach umgangen werden und eine vermeintliche Gesetzeslücke auch ein bewusstes Schweigen des Gesetzgebers darstellen

[897] *Pieroth/Schlink/Kniesel*, POR, § 5 Rn. 19 ff.; *Denninger*, in: Handbuch des Polizeirechts, D Rn. 67; *Tettinger/Erbguth/Mann*, Besonders Verwaltungsrecht, § 15, Rn. 501; vgl. für das Verhältnis von Versammlungsrecht und allgemeinem Polizeirecht: *Kötter/Nolte*, DÖV 2009, 399 (400 f.).

könnte.[898] Zudem hat die zugrundeliegende europäische DSRL eine weitgehend harmonisierende Wirkung.[899] Die von ihr aufgestellten Regelungen dürfen entsprechend nicht durch nationales allgemeines Ordnungsrecht unterlaufen werden. Insbesondere die konkreten Zulässigkeitsvoraussetzungen einer Datenverarbeitung sind von Art. 7 DSRL vollharmonisiert und damit abschließend geregelt.[900] Entscheidend ist indes, ob das allgemeine Datenschutzrecht auch abschließend gegenüber allgemeinen negatorischen Unterlassungs- und Beseitigungsansprüchen anzusehen ist.

Speziell ist zunächst zu untersuchen, ob Anordnungen nach bisheriger Rechtslage gemäß § 38 Abs. 5 BDSG auch an Störer nach dem allgemeinen Ordnungsrecht adressiert werden können oder nur an die verantwortliche Stelle gemäß § 3 Abs. 7 BDSG. *Martini* und *Fritzsche* werfen darüber hinaus die noch weitergehende Frage auf, ob auch Dritte i.S.v. § 3 Abs. 8 BDSG als Adressaten in Betracht kommen.[901] Gleichsam als zivilrechtliches Spiegelbild stellt sich die Frage, ob neben der verantwortlichen Stelle gemäß § 3 Abs. 7 BDSG auch weitere Personen einer zivilrechtlichen Störerhaftung unterliegen können. Hierbei geht es nicht um die Voraussetzungen der Rechtmäßigkeit einer Datenverarbeitung, weshalb Art. 7 DSRL als vollharmonisierende Vorschrift keine Sperrwirkung entfaltet.[902] Entscheidend ist vielmehr, wer für eine nach den Maßstäben von Art. 7 DSRL als rechtswidrig anzuerkennende Datenverarbeitung als Verantwortlicher herangezogen und zu einer Unterlassung derselben verpflichtet werden kann. Es geht somit um die von Art. 7 DSRL nicht geregelte Frage der Rechtsdurchsetzung.

Als Argument für eine abschließende Regelung wird häufig knapp auf den Wortlaut des § 3 Abs. 7 BDSG bzw. des zugrunde liegenden Art. 2 lit. d) DSRL verwiesen: Es sei klar ersichtlich, dass eine Öffnung für weitere Verantwortliche neben der verantwortlichen Stelle nicht vom Gesetzgeber gewünscht gewesen sei.[903] Entsprechend sei es unzulässig, im Rahmen von § 38 Abs. 5 BDSG auf andere Adressaten zurückzugreifen.

---

898 Vgl. allgemein *Pieroth/Schlink/Kniesel*, POR, § 5 Rn. 24.

899 Hierzu bereits ausführlich oben unter C.II.

900 EuGH, *„ASNEF/FECEMD“*, Rs. C-468/10 und C-469/10, Rn. 33 ff. = ZD 2012, 33 (34); vgl. zum Umfang der harmonisierenden Wirkung der DSRL auch bereits oben unter C.II.2. Mit Anwendbarkeit der DS-GVO wird das Argument der harmonisierenden Wirkung noch mehr an Gewicht gewinnen, vgl. nachfolgend unter D.I.3.c)cc)iii).

901 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (13 ff.).

902 Dies verkennt *Gerhold*, ZIS 2015, 156 (160).

903 OVG Schleswig, ZD 2014, 643 (644); VG Schleswig, ZD 2014, 51 (54); *Gerhold*, ZIS 2015, 156 (160); *Piltz*, K&R 2014, 80 (84); *Voigt/Alich*, NJW 2011, 3541 (3543).

Dem ist in dieser Pauschalität nicht zuzustimmen. Am Wortlaut des § 38 Abs. 5 BDSG und dem zugrunde liegenden Art. 24 DSRL fällt zunächst auf, dass dieser – anders als § 7 BDSG und Art. 23 DSRL, welche ausdrücklich die verantwortliche Stelle als Schadensersatzpflichtigen bezeichnen – keinen klaren Adressaten benennt, sondern erfolgsbezogen ausgerichtet ist:[904] Er ermächtigt die Aufsichtsbehörden, zur Gewährleistung der Einhaltung des BDSG und anderer Datenschutzvorschriften Maßnahmen zur Beseitigung festgestellter Verstöße bei der Datenerhebung oder -verarbeitung anzuordnen. In Fällen schwerwiegender Verstöße können sie Datenerhebungen, -verarbeitungen oder -nutzungen untersagen, wenn die Verstöße oder Mängel entgegen einer Anordnung nach § 38 Abs. 5 S. 1 BDSG und trotz eines verhängten Zwangsgeldes nicht in angemessener Zeit beseitigt wurden.

Vereinzelt wird gerade das abgestufte Verfahren als Indiz gegen eine Erweiterung des Adressatenkreises gewertet, da die zunächst anzuordnende Beseitigung der Verstöße und Mängel in der Datenverarbeitung ausschließlich von den Datenverarbeitern vorgenommen werde könne.[905] Auch in der Kommentarliteratur wird ohne nähere Ausführung formuliert, dass die Anordnung gemäß § 38 Abs. 5 S. 1 BDSG gegenüber der verantwortlichen Stelle zu erfolgen habe.[906] Diese Fixierung auf die verantwortliche Stelle scheint indes mehr darin begründet zu sein, dass es erst seit wenigen Jahren überhaupt eine technische Konstellation gibt, in der ein Nicht-Datenverarbeiter potentiell rechtswidrige Datenverarbeitung derart kausal befördern kann, wie es im Falle von Fanpage-Betreibern der Fall ist. Zuvor wäre es gar nicht denkbar gewesen, einen anderen Adressaten als den technisch Verantwortlichen für eine Anordnung heranzuziehen. Speziell im Fall von Fanpages lässt sich jedoch eine Anordnung gegenüber deren Betreibern aussprechen, ein datenschutzkonformes Angebot ihrer Fanpage durch ein entsprechendes Gesuch an den Betreiber des sozialen Netzwerks sicherzustellen oder andernfalls auf die Nutzung der Fanpage zu verzichten.[907]

---

904 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (9 ff.).

905 So OVG Schleswig, ZD 2014, 643 (645).

906 Vgl. beispielsweise *Petri*, in: Simitis, BDSG, § 38 Rn. 73 („Stellt die Aufsichtsbehörde einen technisch-organisatorischen Mangel oder eine Rechtsverletzung fest, ordnet sie gegenüber der verantwortlichen Stelle, in der Regel nach vorheriger Anhörung, die Beseitigung des Mangels an (Satz 1).“), in einem *prima facie* Widerspruch zu *ders.*, in: Simitis, BDSG, § 11 Rn. 21 („Insbesondere Maßnahmen nach § 38 Abs. 5 gegen den Auftragnehmer sind jedoch nicht ausgeschlossen, diese Vorschrift kennt keine Beschränkung aufsichtsbehördlicher Maßnahmen auf verantwortliche Stellen.“); vgl. auch *Brink*, in: Wolff/Brink, § 38 Rn. 76; *Gola/Schomerus*, BDSG, § 38 Rn. 26; *Plath*, in: Plath, § 38 BDSG, Rn. 62.

907 *Petri*, ZD 2015, 103 (105); *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (13).

Der Wortlaut der Regelung ist somit sowohl auf europäischer als auch nationaler Ebene zumindest hinreichend offen, um neben dem datenschutzrechtlich Verantwortlichen die Inanspruchnahme weiterer „Störer“ zu gestatten.[908]

Piltz führt für eine abschließende Regelung der Verantwortlichkeit im Datenschutzrecht ins Feld, dass es eine „unauflösbare Verbindung zwischen einer rechtswidrigen Datenverarbeitung […] und [der] sich erst hieraus ergebenden Haftung“ gebe.[909] Indem nämlich der Schadensersatzanspruch gemäß Art. 23 DSRL bzw. § 7 BDSG ausdrücklich gegen den für die Verarbeitung Verantwortlichen zu richten sei und dieser *a maiore ad minus* auch Unterlassungs- und Beseitigungsansprüche umfasse, spreche sich das Datenschutzrecht dafür aus, dass haftungsbegründende Handlung nur eine rechtswidrige Datenverarbeitung sein könne. Eben diese nehme eine nicht verantwortliche Stelle, die für eine Störerhaftung in Betracht komme, aber nicht vor.[910]

Dem ist entgegenzuhalten, dass das damit implizierte Erfordernis der Eigenhändigkeit der rechtswidrigen Datenverarbeitung bereits der Konzeption der Auftragsdatenverarbeitung gemäß Art. 2 lit. e) i.V.m. Art. 17 Abs. 2 und 3 DSRL bzw. § 11 BDSG widerspricht. Der Auftraggeber einer Auftragsdatenverarbeitung ist hiernach (unmittelbar) verantwortliche Stelle, obwohl seine Handlungen nicht selbst die Qualität einer Datenverarbeitung erreichen. Dieses Minus auf der Handlungsebene wird in der gesetzgeberischen Konzeption dadurch ausgeglichen, dass der Auftraggeber die alleinige Entscheidungskompetenz hinsichtlich der Zwecke und Mittel der Datenverarbeitung sowie eine umfassende Weisungsbefugnis gegenüber dem Auftragnehmer hat.[911] Somit liegt hier eine gesetzliche Zurechnungskonstellation vor.

Auch die DSRL regelt lediglich, dass der für die Verarbeitung Verantwortliche im Falle einer rechtswidrigen Datenverarbeitung einer verschuldensunabhängigen Schadensersatzpflicht unterliegt, vgl. Erwägungsgrund 55 und Art. 23 Abs. 1 DSRL. Eine darüber hinausgehende mittelbare Verantwortlichkeit für Unterlassungs- und Beseitigungsansprüche wird weder ausdrücklich geregelt noch ausgeschlossen. Der von *Piltz* aufgestellte *a maiore ad minus* Schluss[912] ist insoweit keineswegs zwingend, da es sich um unterschiedliche Adressaten

908 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (13); *Kauß*, Revisionsbegründung zum BVerwG, Az. 1 C 28.14 vom 02.01.2015, S. 54.

909 *Piltz*, K&R 2014, 80 (84 f.); In einem Aufsatz aus dem Jahre 2011 ließ er die Anwendbarkeit der zivilrechtlichen Störerhaftung noch offen, vgl. *ders.*, CR 2011, 657 (662 f.).

910 *Piltz*, K&R 2014, 80 (85).

911 *Simitis*, in: Simitis, BDSG, § 11 Rn. 20.

912 *Piltz*, K&R 2014, 80 (84 f.).

handelt: Freilich ist, wer Verpflichteter eines Schadensersatzanspruches ist, erst Recht auch Verpflichteter eines Beseitigungs- und Unterlassungsanspruches. Könnte eine rechtswidrige Datenverarbeitung fortgeführt werden, obwohl hierfür Schadensersatz zu leisten wäre, würde dies dem Grundsatz der Rechtmäßigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 lit. a) DSRL bzw. § 4 Abs. 1 BDSG widersprechen.[913] Dies sagt aber nichts darüber aus, ob eine andere Person, die die höhere Schwelle zum Schadensersatz nicht überschritten hat, nicht dennoch einer niederschwelligeren Pflicht zu Beseitigung oder Unterlassung unterliegen kann. Tatsächlich lässt sich aus dem genannten erst-Recht-Schluss daher nur der Pflichtenumfang des zum Schadensersatz Verpflichteten ableiten. Man könnte sogar so weit gehen, zu konstatieren, dass die aus der Störerhaftung resultierenden Rechtsfolgen der Beseitigung und Unterlassung der Störung gemäß § 1004 Abs. 1 BGB analog dem Datenschutzrecht immanent sind und keine rechtsgebietsfremden Folgen darstellen. Die Störerhaftung wäre somit nicht explizit im Datenschutzrecht geregelt, aber im bestehenden Löschungsrecht und Schadensersatzanspruch angelegt.[914]

Art. 24 DSRL verpflichtet die Mitgliedstaaten zudem, eine „volle Anwendung der Bestimmungen dieser Richtlinie sicherzustellen". Angesichts des in Art. 1 Abs. 1 DSRL erklärten Ziels, den Schutz der Privatsphäre bei der Verarbeitung von personenbezogenen Daten zu gewährleisten, spricht auch dies eher dafür, dass eine Ausweitung der Adressaten von ordnungsrechtlichen Maßnahmen auf weitere „Störer" neben dem für die Verarbeitung Verantwortlichen möglich sein sollte.[915]

In diesem Sinne geht auch die Art. 29 Datenschutzgruppe davon aus, dass Anbieter von Online-Inhalten eine „gewisse Verantwortung" für Datenverarbeitungen haben können, die sie selbst zwar nicht vollständig kontrollieren, wohl aber initiieren, indem sie etwa durch Konfiguration ihrer Webseite eine automatische Weiterleitung der IP-Adresse von Besuchern an die Betreiber von Werbenetzwerken auslösen.[916] Die Anbieter vereinfachten diese Übermittlung und bestimmten die Zwecke mit, nämlich das Versenden gezielter Werbung an die Besucher. Hieraus folge, dass sie „einen Teil der Verantwortung als für die Verarbeitung Verantwortliche"

---

913 *Piltz*, K&R 2014, 80 (84).

914 So trotz einer Ablehnung der Übertragung der Grundsätze der Störerhaftung auch *Piltz*, K&R 2014, 80 (84). *Piltz* ist allerdings im Ergebnis, wenngleich nicht in der Begründung, zuzustimmen, dass die Grundsätze der zivilrechtlichen Störerhaftung nicht herangezogen werden können, um eine ordnungsrechtliche Verantwortlichkeit zu begründen, hierzu sogleich mehr unter D.I.3.c)cc)ii).

915 *Mantz*, ZD 2014, 62 (63 ff.); *Kauß*, Revisionsbegründung zum BVerwG, Az. 1 C 28.14 vom 02.01.2015, S. 51 ff.

916 Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 13 f.

tragen. Diese Verantwortung könne „jedoch nicht die Einhaltung eines Großteils der Verpflichtungen erforderlich machen“, die sich aus der DSRL bzw. der EK-DSRL ergäben.[917] Die Art. 29 Datenschutzgruppe erkennt hiermit an, dass es eine gleichsam abgeschwächte Variante der Verantwortlichkeit gegenüber der unmittelbaren Verantwortung für die Datenverarbeitung geben kann. Diese Form der Verantwortlichkeit zu bestimmen, indem „der Rechtsrahmen flexibel ausgelegt“[918] wird, birgt indes große Rechtsunsicherheiten. Es erscheint damit sowohl rechtssicherer als auch dogmatisch stringenter, diese abgeschwächte Verantwortlichkeit in ein System mittelbarer Haftung, basierend auf dem allgemeinen Haftungsrecht, zu integrieren.

Entgegen der Ansicht des *OVG Schleswig*[919] spricht auch die Gesetzeshistorie tendenziell gegen die Annahme eines abschließenden Charakters der Adressatenregelung in § 38 Abs. 5 BDSG. Mit dem Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.8.2009[920] wurde, zurückgehend auf eine Initiative des Bundesrats[921], erstmals eine Eingriffsmöglichkeit der Aufsichtsbehörden bei materiellen Verstößen gegen das Datenschutzrecht geschaffen. Zuvor war die Anordnungsbefugnis auf die Beseitigung technischer und organisatorischer Mängel beschränkt. Zwar weist das *OVG Schleswig* zutreffend darauf hin, dass sich aus der Gesetzesbegründung keine ausdrückliche Erweiterung des Adressatenkreises auf nicht-verantwortliche Datenverarbeiter und damit Störer im Sinne des Ordnungsrechts ergibt.[922] Dies ist für sich aber noch nicht aussagekräftig, da es 2009 noch kein hinreichend weit verbreitetes Bewusstsein für die sich im Zusammenhang mit sozialen Netzwerken ergebenden Potentiale für Verantwortungsdiffusion und verteilte Datenverarbeitung gegeben haben dürfte. Insbesondere das konkrete Problem von Fanpage-Betreibern, die, ohne selbst Datenverarbeiter zu sein, eine rechtswidrige Datenverarbeitung veranlassen können, dürfte weitgehend unbekannt gewesen sein.[923] Es besteht daher eine Gesetzeslücke, die durch den technischen Fortschritt entstanden ist.[924] Von größerer Bedeutung ist entsprechend der zugrundeliegende Gedanke des Bundesrats, den Aufsichtsbehörden zu ermöglichen, „wirksam präventiv tätig zu

---

917 Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 14; *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (11 f.); *ders./dies.*, VerwArch (104) 2013, 449 (462 f.).
918 Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 14.
919 OVG Schleswig, ZD 2014, 643 (645).
920 BGBl. I, Jg. 2009, S. 2814 ff.
921 Vgl. BT-Drs. 16/12011, S. 44.
922 OVG Schleswig, ZD 2014, 643 (645).
923 Zur Verbreitung und Entwicklung sozialer Netzwerke bereits oben unter B.I.2.; vgl. auch *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (12 f.).
924 Instruktiv zum Problem der Gesetzeslücke *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, S.191 ff.

werden und letztlich den Einsatz einzelner Verarbeitungen zu untersagen, wenn diese materiell rechtswidrig sind".[925]

Auch der teleologische Aspekt eines wirksamen Schutzes personenbezogener Daten spricht gegen eine abschließende Regelung der Störereigenschaft durch das Datenschutzrecht. Während die Nutzer von Fanpages zwar grundsätzlich erkennen können, dass es sich um ein Angebot des sozialen Netzwerkbetreibers handelt, dürften viele eher an ein Angebot des Fanpage-Betreibers denken. Sie vertrauen somit zu einem gewissen Grad darauf, ihre Rechte auch zumindest auch gegenüber diesem durchsetzen zu können, zumal dieser die Möglichkeit hat, für seine Fanpage eine vertrauenswürdige Infrastruktur auszuwählen.[926] Insbesondere wenn es sich um ein deutsches Angebot auf der Fanpage handelt, werden Nutzer auch im Allgemeinen davon ausgehen, dass ihre Daten nach deutschem Datenschutzrecht behandelt werden. Nach vorzugswürdiger Ansicht unterliegt zwar auch das Angebot von Facebook selbst deutschem Datenschutzrecht. Dies ist indes in der instanzgerichtlichen Rechtsprechung umstritten und bisher nicht höchstrichterlich geklärt.[927] Im Sinne eines effektiven Schutzes der informationellen Selbstbestimmung der Nutzer ist daher die Anknüpfung an eine mittelbare Verantwortlichkeit der Fanpage-Betreiber durchaus angezeigt.[928] Dies gilt umso mehr, als wenig einsichtig ist, warum die Fanpage-Betreiber wissentlich auf eine rechtswidrige Infrastruktur zurückgreifen und hieraus Vorteile ziehen dürfen sollten, ohne hierfür zur Verantwortung gezogen zu werden.[929]

Auch die Art. 29 Datenschutzgruppe weist darauf hin, dass sich eine „gewisse Verantwortung für die Datenverarbeitung" für die Anbieter von Online-Inhalten sowohl aus der nationalen Umsetzung der DSRL als auch dem allgemeinen nationalen Recht ergeben könne.[930] Insbesondere Informationspflichten über die Übermittlung von personenbezogenen Daten, aber auch „mögliche weitere Verpflichtungen" könnten sich aus „allgemeinen Rechtsgrundsätzen (Vertrags- und Deliktsrecht) und aus verbraucherschutzrechtlichen Vorschriften" ergeben.[931]

---

925 BT-Drs. 16/12011, S. 44; in diese Richtung auch schon *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (13).

926 *Kauß*, Revisionsbegründung zum BVerwG, Az. 1 C 28.14 vom 02.01.2015, S. 38.

927 Eine Anwendbarkeit deutschen Datenschutzrechts verneinen OVG Schleswig, ZD 2013, 364 (365 f.); VG Schleswig, ZD 2013, 245 (245 ff.); VG Hamburg, ZD 2016, 243 (244 ff.); die Anwendbarkeit bejahen dagegen LG Berlin, ZD 2012, 276 (278); KG Berlin, ZD 2014, 412 (416); ausführlich zu dieser Frage bereits oben unter C.II.

928 *Kauß*, Revisionsbegründung zum BVerwG, Az. 1 C 28.14 vom 02.01.2015, S. 39 f.

929 *Petri*, ZD 2015, 103 (105); *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (11 f.); vgl. auch *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 96.

930 Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 14; vgl. auch *Peifer*, AfP 2014, 18 (20).

931 Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 14, dort Fn. 29.

Die DSRL schließe nicht aus, durch „nationale Rechtsvorschriften eine strafrechtliche oder verwaltungsrechtliche Haftung nicht nur für den für die Verarbeitung Verantwortlichen" vorzusehen, „sondern auch für jede andere Person, die gegen das Datenschutzrecht verstößt".[932] Eine entsprechende strafrechtliche Weitung des Adressatenkreises findet sich national in den §§ 43, 44 BDSG, nach welchen nicht nur die verantwortliche Stelle strafrechtlich zur Verantwortung gezogen werden kann, sondern auch Teilnehmer der Straftat gemäß §§ 26, 27 StGB, ohne dass diese selbst über Mittel und Zwecke der Datenverarbeitung entscheiden könnten.[933] Dies entspricht dem Erwägungsgrund 55 bzw. Art. 24 DSRL, die darauf abzielen, eine umfassende Wirksamkeit der Richtlinie sicherzustellen, indem Sanktionen „jede Person treffen [müssen], die die einzelstaatlichen Voraussetzungen zur Umsetzung dieser Richtlinie nicht einhält."

Den mutmaßlichen gesetzgeberischen Willen zu einem Problem zu ermitteln, das im Zeitpunkt der Verabschiedung der entsprechenden Gesetze technisch noch nicht absehbar war, ist naturgemäß mit einem gewissen spekulativen Element behaftet und stellt entsprechend ein methodisches Problem dar. In Abwägung all der vorgebrachten Argumente ist es aber vorzugswürdig, davon auszugehen, dass eine abschließende Regelung des Adressatenkreises von Unterlassungs- und Beseitigungspflichten angesichts der neuen Verantwortungsdiffusion und Arbeitsteilung im Bereich der Datenverarbeitung nicht intendiert war. Eine abschließende Regelung durch das Datenschutzrecht ist daher sowohl auf bisheriger europäischer als auch nationaler Ebene zu verneinen.

Im Ergebnis sprechen daher die besseren Argumente dafür, die Anwendbarkeit allgemeiner Haftungsgrundsätze neben dem Datenschutzrecht, sowie die Möglichkeit einer mittelbaren Verantwortlichkeit in Bezug auf Beseitigungs- und Unterlassungsansprüchen grundsätzlich zu bejahen.[934] In einem nächsten Schritt ist zu klären, unter welchen Voraussetzungen eine solche mittelbare Verantwortlichkeit anzunehmen ist.

---

932 Art. 29 DatSchGruppe, Stellungnahme 1/2010, WP 169, S. 20, dort Fn. 15; vgl. auch *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 94, 96, die die Anwendbarkeit „allgemeiner Rechtsgrundsätze" zur Bestimmung der Verantwortlichkeit betonen.

933 *Mantz*, ZD 2014, 62 (64).

934 Vgl. auch *Spindler*, GRUR-Beilage 2014, 101 (108); *Schulz/Hoffmann*, in: PdK, Band L 16 Bund Rn. 94, 96; a.A. *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (11), die die datenschutzrechtlichen Voraussetzungen als maßgeblich für die Verhaltenszurechnung ansehen, sich mit der Frage des abschließenden Charakters des Datenschutzrechts allerdings nicht vertieft auseinandersetzen.

ii) Umfang und Voraussetzungen mittelbarer Verantwortlichkeit von Fanpage-Betreibern

Eine mittelbare Verantwortlichkeit im Datenschutzrecht muss sich in engen Grenzen bewegen, damit sie operationalisierbar bleibt und nicht zu einer unbegrenzten Ausuferung der Haftung führt. Sie beschränkt sich auf negative Unterlassungs- und Beseitigungsansprüche, da die positiven datenschutzrechtlichen Pflichten abschließend an die unmittelbar verantwortliche Stelle gemäß § 3 Abs. 7 BDSG adressiert sind. Insbesondere mit Blick auf den Grundsatz der Bindung der Verwaltung an das Gesetz gemäß Art. 20 Abs. 3 GG stellt sich dennoch die Frage der gesetzlichen Anknüpfung. In Betracht kommt entweder eine Herleitung aus einer allgemeinen Auswahlverantwortung bei einer Aufgabenübertragung[935] (hierzu sogleich (1)) oder aber unter Rückgriff auf die allgemeinen ordnungsrechtlichen Grundsätze des Zweckveranlassers (hierzu nachfolgend unter (2)).

Eine mögliche Verbindung von zivilrechtlicher Störerdogmatik und dem Datenschutzrecht – wie vereinzelt diskutiert[936] – ist dagegen nicht geeignet, um eine ordnungsrechtliche Verantwortlichkeit zu begründen. Die hierüber geführte Diskussion ist vielmehr dahingehend einzuordnen, ob aus datenschutzrechtlichen Regelungen eine zivilrechtliche Haftung begründet werden kann; nicht aber, ob der zivilrechtliche Störerbegriff haftungsbegründend im öffentlichen Recht wirken kann. Auf die Frage der zivilrechtlichen mittelbaren Verantwortlichkeit soll hier daher nur ausblicksartig unten unter (3) nach Klärung der ordnungsrechtlichen Verantwortlichkeit eingegangen werden.

(1) Auswahlverantwortlichkeit gemäß § 11 Abs. 2 S. 1 i.V.m. § 4 BDSG

Martini und *Fritzsche* haben sich detailliert und sehr präzise mit den Problemen der möglichen Schutzlücken und der Umgehungsanreize für Fanpage-Betreiber auseinandergesetzt, die aus der fehlenden unmittelbaren datenschutzrechtlichen Verantwortlichkeit resultieren, sowie mit den Möglichkeiten einer mittelbaren Verantwortungszuweisung.[937] Die von ihnen präsentierte Lösung ist die Annahme einer „Auswahlverantwortlichkeit" desjenigen, der sich eines Dritten bedient, um im eigenen Interesse Datenverarbeitungen vornehmen zu lassen. Diese ergebe sich in einem *a maiore ad minus* Schluss aus § 11 Abs. 2 S. 1 i.V.m. § 4 BDSG: Das Gesetz erlege dem Auftraggeber einer Auftragsdatenverarbeitung strenge Auswahlpflichten auf, deren Verletzung gemäß § 43 Abs. 1 Nr. 2b BDSG mit einem Bußgeld geahndet werden könne. Es

935 So zuerst *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (11 ff.).
936 *Piltz*, K&R 2014, 80 (83 ff.); *Mantz*, ZD 2014, 62 (63 ff.); *Spindler*, GRUR Beilage 2014, 101 (108).
937 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (9 ff.).

sei daher nicht einsichtig, dass ein Diensteanbieter, der sich nicht eines Auftragnehmers, sondern eines Dritten bediene, der noch größere Freiheiten in der Datenverarbeitung habe, weniger strengen Anforderungen an die Auswahl unterliegen solle.[938] Vielmehr wolle das Gesetz „[j]ede Form der Einschaltung Dritter für Datenverarbeitungen […] sehr strengen Schranken unterwerfen, insbesondere Umgehungen des gesetzlichen Schutzinstrumentariums einen Riegel vorschieben."[939]

Funktion des § 11 BDSG ist insbesondere eine Privilegierung des Datenaustausches zwischen Auftraggeber und Auftragnehmer: Sofern die strengen Voraussetzungen der Auftragsdatenverarbeitung eingehalten werden, ist eine Übermittlung von Daten zwischen den Partnern ohne weitere rechtliche Beschränkungen zulässig, da sie gemäß § 3 Abs. 8 S. 3 BDSG zueinander nicht als Dritte einzustufen sind.[940] Die Auftragsdatenverarbeitung steht im Gegensatz zur bloßen Funktionsübertragung, bei welcher ein Dritter beauftragt wird, eigenverantwortlich vom ursprünglichen Datenverarbeiter übermittelte Daten zu verarbeiten.[941] Es ist *Martini* und *Fritzsche* uneingeschränkt zuzustimmen, dass beide Konstellationen in Bezug auf Fanpage-Betreiber nicht vorliegen, da es einerseits an einem Auftragsverhältnis Facebook gegenüber mangelt und andererseits die Nutzer selbst die Daten an Facebook übermitteln, ohne den Umweg über den Fanpage-Betreiber zu nehmen.[942]

Hieraus lässt sich aber nicht der Schluss ziehen, dass „eine Verarbeitung durch einen Dritten, die nicht mit einer Übermittlung einhergeht", aber dennoch im Interesse hier des Fanpage-Betreibers erfolgt, erst Recht strengen Bindungen unterworfen sein muss und dies vom normativen Programm des Gesetzgebers „in der Sache mitgedacht" sei.[943] Tatsächlich handelt es sich um eine zwar ähnliche, aber dennoch grundlegend andere Situation. Ein Auftraggeber ist kraft seiner umfassenden Entscheidungsbefugnis hinsichtlich der Mittel und Zwecke der Datenverarbeitung stets selbst datenschutzrechtlich verantwortlich gemäß § 3 Abs. 7 BDSG.[944] Dasselbe gilt für einen Datenverarbeiter, der im Rahmen einer Funktionsübertragung Daten an

938 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (12).
939 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (12).
940 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (12); vgl. auch *Petri*, in: Simitis, BDSG, § 11 Rn. 22; *Spoerr*, in: Wolff/Brink, § 11 BDSG, Rn. 4, 34; *Plath*, in: Plath, § 11 BDSG, Rn. 4; *Koós/Englisch*, ZD 2014, 276 (277); *Roßnagel/Kroschwald*, ZD 2014, 495 (497); zur Auftragsdatenverarbeitung auch bereits oben unter D.I.2.a).
941 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (6 f.; 12); instruktiv zum Begriff der Funktionsübertragung *Spindler/Nink*, in: Spindler/Schuster, § 11 BDSG Rn. 13; *Petri*, in: Simitis, BDSG, § 11 Rn. 22 ff.; *Gola/Schomerus*, § 11 Rn. 9.
942 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (12); vgl. auch bereits oben unter D.I.3.c)bb).
943 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (12).
944 *Petri*, in: Simitis, BDSG, § 11 Rn. 1, 22, 48; *Spoerr*, in: Wolff/Brink, § 11 BDSG, Rn. 34.

einen Dritten gemäß § 3 Abs. 4 Nr. 3 BDSG übermittelt.[945] Beiden Konstellationen ist mithin gemein, dass Regelungen für den Fall getroffen werden, dass eine bereits datenschutzrechtlich verantwortliche Stelle sich zur Erreichung und Umsetzung ihrer Interessen einer anderen Stelle bedient, an diese Daten übermittelt und die anschließend gewünschten Datenverarbeitungsschritte nicht eigenhändig vornimmt. Es besteht eine vollständige Übereinstimmung mit der Regelung des § 3 Abs. 7 BDSG, ggf. in richtlinienkonformer Auslegung gemäß Art. 2 lit. d) DSRL.[946] § 11 i.V.m. § 3 Abs. 8 S. 3 BDSG lässt sich insoweit nicht nur als Privilegierung verstehen, sondern zugleich als Klarstellung, dass die zuvor bestehende datenschutzrechtliche Verantwortlichkeit des Auftraggebers auch im Rahmen der Auftragsdatenverarbeitung kraft seiner Kontrolle über den Auftragnehmer bei ihm verbleibt. Die darüber hinausgehende Auswahlverantwortlichkeit des Auftraggebers ist nicht konstitutiv für seine eigene datenschutzrechtliche Verantwortlichkeit, sondern nur für den Erwerb der privilegierten Datenübermittlung an den zukünftigen Auftragnehmer.

An eben dieser eigenen originären datenschutzrechtlichen Verantwortlichkeit gemäß § 3 Abs. 7 BDSG mangelt es bei dem Betreiber einer Fanpage. Eine allgemeine Auswahlverantwortlichkeit würde damit nicht verantwortlichkeits-modifizierend, sondern vielmehr verantwortlichkeits-begründend wirken. Es überzeugt daher nicht, dass die Auswahlverantwortlichkeit des Fanpage-Betreibers „in der Konsequenz des gesetzlichen Regelungskonzepts“ liege und keine „Ausweitung von Befugnissen über den Tatbestand hinaus“ darstelle.[947] Wiewohl das Ergebnis im Hinblick auf eine effektive Durchsetzung des Datenschutzrechts angesichts der herausgearbeiteten Regelungslücke zu begrüßen ist, stellt es eine belastende verwaltungsrechtliche Analogie dar.[948] Eine solche ist indes aufgrund des Vorbehalts des Gesetzes gemäß Art. 20 Abs. 3 GG, wonach die Eingriffsbefugnisse der Exekutive durch ein ermächtigendes Gesetz hinreichend bestimmt und begrenzt sein müssen, unzulässig.[949] Eine behördliche Handlung, die auf Grund einer solchen Analogie vorgenommen wird, stellt einen Eingriff in die allgemeine Handlungsfreiheit gemäß Art. 2 Abs. 1 GG i.V.m. dem Rechtsstaatsprinzip dar, der nicht durch ein entsprechendes Gesetz legitimiert ist.[950]

945 Vgl. *Spindler/Nink*, in: Spindler/Schuster, § 11 BDSG Rn. 13.
946 Zum Begriff der verantwortlichen Stelle bereits ausführlich oben unter C.II.4.
947 So aber *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (12).
948 a.A. ausdrücklich *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (12).
949 BVerfG, NJW 1996, 3146 (3146).
950 BVerfG, NJW 1996, 3146 (3146).

Selbst wenn man ein generelles Analogieverbot im Bereich der Eingriffsverwaltung ablehnt[951], ist eine solche jedenfalls restriktiv zu handhaben und kommt im Falle einer Grundrechtsbeeinträchtigung nur dann in Frage, wenn keine andere Möglichkeit besteht, die eigentlich zuständige Stelle zur Wahrnehmung ihrer Aufgaben zu bewegen.[952] Auch diese Ausnahme würde bei einer Verfügung gemäß § 38 Abs. 5 BDSG analog gegenüber Fanpage-Betreibern – die hierdurch zumindest in ihrer allgemeinen Handlungsfreiheit und gegebenenfalls auch ihrer Berufsfreiheit beschränkt würden – nicht vorliegen: Zum einen geht es schon formal nicht darum, eine bestehende Eingriffsermächtigung einer anderen Behörde zu nutzen und damit lediglich die Zuständigkeit analog zu begründen, sondern um die materielle Erweiterung der Eingriffsgrundlage. Zum anderen können gerade bei Facebook-Fanpages ordnungsrechtliche Verfügungen an Facebook selbst adressiert werden, so dass keine Gefahr eines vollständigen Vollzugsdefizits besteht.

Eine mittelbare Verantwortlichkeit der Fanpage-Betreiber aufgrund einer vermeintlichen Auswahlverantwortlichkeit gemäß § 11 Abs. 2 S. 1 i.V.m. § 4 BDSG ist daher als unzulässige belastende verwaltungsrechtliche Analogie abzulehnen.

(2) Mittelbare Verantwortlichkeit als Zweckveranlasser

Eine mittelbare Verantwortlichkeit der Fanpage-Betreiber für die rechtswidrige Verarbeitung von Bestands- und Nutzungsdaten durch Facebook, von der sie u.a. durch die anonym zur Verfügung gestellten Nutzerstatistiken profitieren, lässt sich aber unter Rückgriff auf das allgemeine Polizei- und Ordnungsrecht begründen. Dieses ist freilich nur in dem Maße anwendbar, wie das Datenschutzrecht keine Sperrwirkung als besonderes Ordnungsrecht entfaltet.[953] Wie oben unter D.I.3.c)cc)i) dargelegt, ist das Datenschutzrecht indes nicht als abschließend auszulegen, soweit Beseitigungs- und Unterlassungspflichten betroffen sind. Insbesondere § 38 Abs. 5 BDSG ist, ebenso wie die zugrundeliegenden Regelungen der DSRL, in seinem Regelungsgehalt offen genug, um einen solchen Rückgriff zu gestatten. Da es sich bei dem allgemeinen Polizei- und Ordnungsrecht um gesetzlich hinreichend legitimierte Eingriffsbefugnisse handelt, besteht auch kein Problem mit dem verwaltungsrechtlichen Analogieverbot.

---

951 So *Sachs*, in: Stelkens/Bonk/Sachs, VwVfG, § 44 Rn. 54 m.w.N.

952 *Sachs*, in: Stelkens/Bonk/Sachs, VwVfG, § 44 Rn. 54 m.w.N.; BVerfG, NJW 1999, 3404 (3405).

953 Vgl. zum Spezialitätsgrundsatz im Verwaltungsrecht *Pieroth/Schlink/Kniesel*, POR, § 5 Rn. 19 ff.; *Denninger*, in: Handbuch des Polizeirechts, D Rn. 67; *Tettinger/Erbguth/Mann*, Besonders Verwaltungsrecht, § 15, Rn. 501; *Kötter/Nolte*, DÖV 2009, 399 (401).

Die Fanpage-Betreiber sind – anders als Facebook selbst – keine unmittelbaren Störer im Sinne der Theorie der unmittelbaren Verursachung, da ihr eigenes Verhalten nach wertender Betrachtung nicht die Grenze zu einer konkreten Gefahr für ein ordnungsrechtlich geschütztes Rechtsgut überschreitet.[954] Obwohl die Abgrenzung zwischen unmittelbarer und mittelbarer Verantwortlichkeit im Einzelfall unscharf sein kann[955], ist daher festzuhalten, dass insoweit keine unmittelbare ordnungsrechtliche Verantwortlichkeit der Fanpage-Betreiber besteht.

Herrschend ist – insbesondere von der Rechtsprechung – über den unmittelbar Verantwortlichen hinaus die Figur des Zweckveranlassers anerkannt.[956] Dieser verursacht die unmittelbare Gefahr zwar nicht selbst, führt sie aber letztlich herbei. Zwischen seinem Verhalten und dem gefahrverursachenden Verhalten Dritter besteht somit ein derart enger innerer Zusammenhang, dass er sich die Gefahr selbst zurechnen lassen muss.[957] In der Literatur wird hieran verbreitet starke Kritik geübt: Abgesehen davon, dass es keine klare Stütze im Gesetz gebe, handele es sich um eine zu Rechtsunsicherheit führende Modifizierung der Lehre der unmittelbaren Verursachung, die legales Verhalten aufgrund von subjektiven Unterstellungen unzulässig und in unvorhersehbarer Weise beschränke.[958]

Diese Kritik ist überzogen. Die Theorie der unmittelbaren Verursachung stellt – auch nach Verständnis der Kritiker – nicht das Erfordernis auf, dass „Unmittelbarkeit" stets im Sinne einer zeitlichen Letztverursachung zu verstehen sei.[959] Vielmehr handelt es sich um ein normatives Merkmal, das entsprechend einer wertenden Auslegung im Einzelfall zugänglich ist. Wäre nur die zeitlich letzte Ursache ordnungsrechtlich relevant, käme es zu erheblichen Schutzdefiziten. Die alternativ vertretene Lehre von der Sozialadäquanz[960] und die Rechtswidrigkeitslehre[961] bieten zwar dogmatische Rechtssicherheit, da nach ihnen Störer nur ist, wer gegen eine Rechts- bzw. Sozialnorm verstößt und hierzu nicht durch eine andere Rechtsnorm befugt ist. Auch diese Auslegung kann in der sich immer schneller wandelnden Welt indes zu massiven Schutzlücken

954 *Pieroth/Schlink/Kniesel*, POR, § 9 Rn. 15; *Gusy*, POR, Rn. 335; *Tettinger/Erbguth/Mann*, Besonderes Verwaltungsrecht, § 15 Rn. 491; *Denninger*, in: Handbuch des Polizeirechts, D Rn. 77. Zur Frage der unmittelbaren Verantwortlichkeit der Fanpage-Betreiber bereits ausführlich oben unter D.I.3.c)bb).

955 *Pieroth/Schlink/Kniesel*, POR, § 9 Rn. 19; entsprechend kritisch *Gusy*, POR, Rn. 336 f.; *Denninger*, in: Handbuch des Polizeirechts, D Rn. 77 ff.

956 BVerwG, DVBl. 1989, 59 (60); OVG Koblenz, DVBl. 2012, 515 (519) m.w.N.; *Schenke*, POR, § 4 Rn. 244 ff. m.w.N.; *Schoch*, Jura 2009, 360 (361).

957 *Schenke*, POR, § 4 Rn. 244 ff. m.w.N.; *Schoch*, Jura 2009, 360 (361).

958 *Pieroth/Schlink/Kniesel*, POR, § 9 Rn. 29; *Gusy*, POR, Rn. 336 ff.; *Denninger*, in: Handbuch des Polizeirechts, D Rn. 77 ff., jeweils m.w.N.

959 *Schenke*, POR, § 4 Rn. 244; *Schoch*, Jura 2009, 360 (361); vgl. auch *Pieroth/Schlink/Kniesel*, POR, § 9 Rn. 13 f.; *Gusy*, POR, Rn. 335 f.

960 Instruktiv: *Gusy*, POR, Rn. 339 m.w.N.

961 *Denninger*, in: Handbuch des Polizeirechts, D Rn. 81 ff. m.w.N.

führen und lädt zudem förmlich zu Umgehungskonstruktionen ein. Zudem wird sie insbesondere der Schutzpflichtdimension der Grundrechte und dem Ziel der Gewährleistung eines effektiven Grundrechtsschutzes nicht gerecht. Hierauf wird sogleich zurückzukommen sein. Die Figur des Zweckveranlassers ist daher grundsätzlich anzuerkennen.

Das Verhalten der Fanpage-Betreiber trägt in einer nach diesen Grundsätzen zurechenbaren Weise zu Facebooks Überschreiten der ordnungsrechtlichen Gefahrenschwelle bei.[962] Dies gilt unabhängig davon, ob man den Zweckveranlasser objektiv oder subjektiv bestimmt, so dass es dahinstehen kann, welcher dieser Theorien zu folgen ist.[963] Aus den Medien und datenschutzbehördlichen Verfahren ist bekannt, dass jedenfalls starke Zweifel an der Rechtmäßigkeit des Umgangs Facebooks mit Nutzungs- und Bestandsdaten bestehen. Da diese Daten zwingend beim Besuch einer Fanpage durch Nutzer anfallen, ist die hieraus resultierende Gefahr für ihre informationelle Selbstbestimmung aus der Sicht eines unbeteiligten Dritten objektiv eine typische Folge des Betriebs der Fanpage. Wie oben bereits dargestellt, ist es zudem essentieller Teil des Geschäftsmodells Facebooks, von Nutzern gewonnene Daten auszuwerten um zielgruppenorientierte Werbung vermarkten zu können. Fanpages stellen hierbei einen wichtigen Bestandteil dar, da sie das Netzwerk mit Inhalten füllen und Nutzer somit dazu anregen, es zu nutzen und dadurch Daten zu produzieren.[964] Auch dieser Zusammenhang ist für einen objektiven Dritten erkennbar. Indem die Fanpage-Betreiber das Datenaufkommen in dem sozialen Netzwerk erhöhen und Nutzer zu einer breiteren Verwendung ermutigen, fördern und ermöglichen sie zurechenbar die Datenschutzverstöße durch Facebook.[965]

Auch subjektiv nehmen die Fanpage-Betreiber jedenfalls billigend in Kauf, dass es zu einer rechtswidrigen Datenverarbeitung kommt. Sie können von den rechtlichen Zweifeln an Facebooks Datenverarbeitung über die Medien Kenntnis nehmen und profitieren darüber hinaus direkt von der anonymisierten Statistik „Insights“, welche bei ihrer Erstellung jedenfalls teilweise auf die anfallenden Bestands- und Nutzungsdaten zurückgreift, um z.B. Alter und Geschlecht der Seitennutzer zu bestimmen. Zudem akzeptieren und billigen sie mit den AGB

962 So auch *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (10).

963 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (10); instruktiv: *Schenke*, POR, § 4 Rn. 244 f.; *Schoch* , Jura 2009, 360 (363).

964 *Kauß*, Revisionsbegründung zum BVerwG, Az. 1 C 28.14 vom 02.01.2015, S.65 f.; *Caspar*, ZD 2015, 12 (13); *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (3, 10); *ders./dies.*, VerwArch (104) 2013, 449 (453 f.); *Weichert*, ZD 2014, 605 (608).

965 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (10).

und Datenrichtlinien Facebooks auch die dort aufgeführten datenschutzwidrigen Regelungen.[966]

Einer mittelbaren Verantwortlichkeit als Zweckveranlasser steht auch nicht entgegen, dass die Fanpage-Betreiber ihrerseits eigene Grundrechte rechtmäßig ausüben. Für hoheitliche Fanpage-Betreiber folgt dies bereits daraus, dass diese sich als staatliche Akteure grundsätzlich nicht auf Grundrechte berufen können.[967] Sie sollen im folgenden Abschnitt unter D.I.3.c)dd) noch gesondert betrachtet werden.

Bei privaten Akteuren gestaltet sich die Situation komplizierter. Grundsätzlich gilt, dass derjenige, der als Privater eigene Rechte ausübt und somit ein von der Rechtsordnung toleriertes Risiko setzt, hierbei kein ordnungsrechtlicher Störer sein kann.[968] Wann dies noch der Fall ist, unterliegt freilich durch die Figur des Zweckveranlassers einer stark normativen Betrachtung. Dies stellt auch den zentralen Ansatzpunkt für die zuvor beschriebene grundsätzliche Kritik an dieser Figur dar.

Das Betreiben von Fanpages ist allgemein ein legales Verhalten. Es führt keinesfalls zwangsläufig zu einer Gefährdung von geschützten Rechtsgütern. Im Falle von Facebook Fanpages existiert allerdings, wie dargelegt, ein sehr enger Zusammenhang zwischen dem Betrieb der Fanpage, einer dadurch ermöglichten rechtswidrigen Datenverarbeitung durch Facebook und hieraus gewonnenen Vorteilen der Fanpage-Betreiber. Die Vorteile können von den Fanpage-Betreibern auch nicht abbestellt werden – sie können sich allenfalls entscheiden, einige von diesen, etwa die anonyme Nutzerstatistik, nicht aktiv zu nutzen.[969] Selbst dann profitieren sie aber immer noch von der erhöhten Reichweite ihres Angebots. Es kann entsprechend bereits mit gutem Recht bezweifelt werden, ob das Betreiben einer solchen Fanpage auf Facebook tatsächlich vollkommen sozialadäquat ist. Zudem ist es der Zweckveranlassung immanent, dass auch für sich genommen rechtlich neutrales Verhalten zu einer Qualifizierung als Störer führen kann, wenn eine hieraus resultierende Gefahr hinreichend absehbar ist. Wäre der Maßstab so streng wie beim regulären Handlungsstörer, würde sich der Rückgriff auf diese Figur erübrigen. Zutreffenderweise wird insofern darauf verwiesen, dass es

966 *Caspar*, ZD 2015, 12 (13 f.); *Kauß*, Revisionsbegründung zum BVerwG, Az. 1 C 28.14 vom 02.01.2015, *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (10); S. 59 ff.; *Karg/Thomsen*, DuD 2012, 729 (731); vgl. zu den Vorteilen von Fanpages für Unternehmen ausführlich *Lichtnecker*, GRUR 2013, 135 (136 f.).

967 Vgl. hierzu allgemein *Herdegen*, in: Maunz/Dürig, GG, Art. 1 Abs. 3 Rn. 51.

968 *Pieroth/Schlink/Kniesel*, POR, § 9 Rn. 17; *Gusy*, POR, Rn. 339; *Schenke*, POR, § 4 Rn. 243; *Denninger*, in: Handbuch des Polizeirechts, D Rn. 79; *Tettinger/Erbguth/Mann*, Besonderes Verwaltungsrecht, § 15 Rn. 493.

969 Vgl. *Karg/Thomsen*, DuD 2012, 729 (731).

sich bereits bei der Bestimmung der Zweckveranlassung um ein „Wertungsproblem“ handelt, für dessen Lösung auf den Grundsatz der Verhältnismäßigkeit zurückzugreifen sei.[970] Freilich hinge eine solche Verhältnismäßigkeitsprüfung aber in der Luft, würde sie nicht zunächst durch eine Gegenüberstellung der Grundrechtspositionen unter Rückgriff auf die allgemeine Grundrechtsdogmatik vorbereitet. Um die Grenzen des rechtlich erlaubten Risikos zu bestimmen, ist es daher erforderlich, die Grenzen der jeweils betroffenen Grundrechte zu bestimmen.

Dass eine Person, die lediglich ihre eigenen Rechte ausübt, kein Handlungsstörer sein kann, ist grundrechtlich dadurch bedingt, dass diese Person einen Freiraum nutzt, welcher der exekutiven Gewalt entzogen sein soll. Auf dieser grundrechtlichen Ebene realisieren die Betreiber von Fanpages, soweit sie Deutsche sind, ihre Berufsfreiheit gemäß Art. 12 GG bzw. ihre allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG, soweit sie Nicht-EU-Ausländer sind.

Ebenfalls auf dieser grundrechtlichen Ebene liegt allerdings auch die informationelle Selbstbestimmung der Nutzer gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, welche durch die Fanpages gefährdet wird. Natürlich tangiert dies die Fanpage-Betreiber zunächst nicht direkt, da es keine unmittelbare Drittwirkung von Grundrechten unter Privaten gibt. Es ist aber allgemein anerkannt, dass die informationelle Selbstbestimmung über eine starke Schutzpflichtdimension verfügt, die zu einer mittelbaren Drittwirkung gegenüber Privaten führt.[971] Kernbestandteil dieser Schutzpflicht als staatliche Verantwortung ist – mit den Worten des Bundesverfassungsgerichts – „die Voraussetzungen selbstbestimmter Kommunikationsteilhabe zu gewährleisten.“[972] Die Sicherung innerer und äußerer Verhaltensfreiheit, welcher die informationelle Selbstbestimmung instrumentell dient,[973] kann nur gelingen, wenn es dem Einzelnen grundsätzlich möglich ist nachzuvollziehen, gegenüber wem und in welchem Zusammenhang seine persönlichen Daten offenbart werden.[974] Informationeller Selbstschutz muss dem Einzelnen „tatsächlich möglich und zumutbar“ sein,

970 *Schenke*, POR, § 4 Rn. 246; *Denninger*, in: Handbuch des Polizeirechts, D Rn. 80.

971 BVerfGE 117, 202 (227 f.), Rn. 62 f. – Vaterschaftstest; BVerfGK 9 353 (358) - Schweigepflichtentbindung; *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 189; *Sandfuchs*, Privatheit wider Willen, S. 131 ff.; *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 585 ff.; *Hoffmann-Riem*, AöR 1998, 513 (522 ff.); *Kühling*, Die Verwaltung (44) 2011, 525 (551).

972 BVerfGK 9 353 (358) – Schweigepflichtentbindung; vgl. auch BVerfGE 117, 202 (226), Rn. 60 f. – Vaterschaftstest.

973 Ausführlich *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 569 ff., 573.

974 Grundlegend BVerfGE 65, 1 (43) – Volkszählung; *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 175; *Sandfuchs*, Privatheit wider Willen, S. 132 f.); *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 577; *Masing*, NJW 2012, 2305 (2308).

ein bloßer Verweis auf eine „nur scheinbare Freiwilligkeit der Preisgabe bestimmter Informationen“ verfehlt die staatliche Schutzpflicht.[975] Dies entspricht dem allgemeinen Grundsatz, dass einer Schutzpflicht nur dann Genüge getan ist, wenn der vermittelte Schutz auch tatsächlich wirksam ist.[976] Die Figur des Zweckveranlassers als Teil des Ordnungsrechts erweist sich insoweit als ein geeignetes Instrument, um diese Schutzpflicht umzusetzen.

Die Gefährdung der informationellen Selbstbestimmung der Nutzer durch den Betrieb von Fanpages wurde bereits umfassend dargelegt. Die Setzung des datr-Cookies und die aus der Reichweitenanalyse ermöglichte umfassende Profilbildung durch Facebook erweisen sich insbesondere deshalb als eingriffsintensiv, weil sie ohne Wissen und Kontrolle des Nutzers und teilweise sogar Nichtnutzers geschehen.[977] Die Betroffenen haben keine anderen Selbstschutzmöglichkeiten gegen diese Form der Datenverarbeitung, außer gänzlich auf den Besuch der Fanpage zu verzichten. Sogar diese Option zum Selbstschutz erweist sich als wirkungslos, wenn den Nutzern wegen einer mangelnden Kenntnis von der Datenverarbeitung und fehlendem Interesse an datenschutzbehördlichen Verfahren gegen Facebook gar nicht bewusst ist, dass ein solcher Verzicht ratsam wäre. Angesichts dieser erheblich eingeschränkten Möglichkeiten zum Selbstschutz ist daher davon auszugehen, dass hier eine staatliche Schutzpflicht besteht, um die Voraussetzungen für wirkungsvollen Selbstschutz zu schaffen.

Das bloße Bestehen einer Schutzpflicht führt freilich nicht unmittelbar zu einer ordnungsrechtlichen Beschränkbarkeit der Freiheiten der privaten Fanpage-Betreiber. Vielmehr bestünde dann die Gefahr eines Zirkelschlusses, da die Rechtmäßigkeit ordnungsrechtlichen Einschreitens aus einer vermeintlichen Notwendigkeit derselben hergeleitet würde. Wie für jeden staatlichen Eingriff ist daher eine gesonderte Ermächtigungsgrundlage erforderlich.[978] Eine solche existiert allerdings mit § 38 Abs. 5 BDSG i.V.m. den allgemeinen Grundsätzen der Zweckveranlassung. Die hier interessierende Frage ist daher, ob sich aus der bestehenden Schutzpflicht gegenüber den Nutzern eine Einstufung der Fanpage-Betreiber als Zweckveranlasser rechtfertigen lässt, obwohl diese ihrerseits eigene Freiheiten ausüben und sich rechtlich im Grundsatz neutral verhalten.

---

975 BVerfGK 9 353 (358 f.) – Schweigepflichtentbindung; vgl. auch *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 588; *Gusy*, DuD 2009, 33 (37 f.).

976 BVerfGE 88, 203 (255), Rn. 158 f. – Schwangerschaftsabbruch II.

977 Ausführlich oben unter B.II.2.b)aa) und B.II.3.b)bb). Zur Erinnerung: Ein Aufruf einer Facebook Fanpage ist in aller Regel möglich, ohne sich in dem sozialen Netzwerk anzumelden oder zu registrieren. Lediglich zur Nutzung der Kommentarfunktion ist eine Anmeldung erforderlich.

978 *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 189.

Die Existenz der staatlichen Schutzpflicht im Bereich von Fanpages zeigt, dass es sich bei diesen um grundrechtsgefährdende Angebote handelt, deren Gefahren die Mehrheit der Nutzer nicht selbst wirksam entgegen treten kann. Der Staat kann seiner Schutzpflicht natürlich auf verschiedene Art und Weise nachkommen, beispielsweise auch durch Bildungsmaßnahmen für die Nutzer, also nicht nur durch eine Beschränkung des Betriebs von Fanpages. Gleichzeitig erscheint es aber wenig überzeugend, dass der Betrieb einer solchen Fanpage, wenn er sogar staatliche Schutzpflichten auslöst, ein rechtlich vollkommen toleriertes und sozial akzeptiertes Risiko darstellt.[979]

Dies ist in der notwendigen Verhältnismäßigkeitsprüfung bei der Bestimmung der Zweckveranlassung[980] zu berücksichtigen. Eine Einordnung der Betreiber von Fanpages als Zweckveranlasser mit der Folge, dass gemäß § 38 Abs. 5 BDSG Untersagungsverfügungen hinsichtlich des Betriebs der Fanpage an sie gerichtet werden könnten, beschränkt die hinter ihnen stehenden Unternehmen und Privatpersonen in ihren Möglichkeiten, Aufmerksamkeit und Reichweite für ihre Waren, Dienstleistungen und auch nichtkommerziellen Projekte zu erhalten und damit gegebenenfalls in ihrer Berufsfreiheit nach Art. 12 Abs. 1 GG bzw. ihrer allgemeinen Handlungsfreiheit nach Art. 2 Abs. 1 GG. Eine solche Einschränkung kann sich ökonomisch negativ auf sie auswirken, wenn deswegen Umsatzeinbußen zu verzeichnen sind. Allerdings gibt es andere Möglichkeiten der Werbung und des Marketings, die nicht zwingend die Gefahr einer rechtswidrigen Datenverarbeitung durch Facebook in sich bergen. Hierzu zählt entweder das Ausweichen in andere, datenschutzkonformere soziale Netzwerke[981] oder das Betreiben einer eigenen Webseite, auf der – wenn denn gar nicht auf Facebook verzichtet werden soll – gegebenenfalls ein datenschutzkonform gestaltetes Social PlugIn, etwa in Form der Zwei-Klick-Lösung, verwendet wird.[982]

Dem steht die dargelegte erhebliche Gefährdung der informationellen Selbstbestimmung der Nutzer, verbunden mit ihren sehr eingeschränkten Selbstschutzmöglichkeiten, gegenüber. Gerade Nutzern, die nicht selbst bei Facebook angemeldet sind, sondern sich nur für das ohne

---

979 Bezüglich der grundsätzlichen Zurechenbarkeit zustimmend, diese aber aufgrund des vermeintlich abschließenden Charakters des Datenschutzrechts als Sonderordnungsrecht ablehnend: *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (10 f.).

980 Vgl. *Schenke*, POR, § 4 Rn. 246; *Denninger*, in: Handbuch des Polizeirechts, D Rn. 80.

981 Wenngleich hierbei durch die marktbeherrschende Stellung Facebooks natürlich weniger potentielle Adressaten erreicht werden könnten und die Effektivität eines solchen Marketings damit reduziert wäre. Allein daraus, dass die Nutzung Facebooks effizient ist, lässt sich indes nicht rechtfertigen, diese Reichweite auch unter der Verletzung von Betroffenenrechten in Anspruch zu nehmen. Dies gilt umso mehr, als ein nicht unerheblicher Teil dieser Effizienz – wie oben gezeigt – durch Verletzung eben dieser Betroffenenrechte erzielt wird.

982 Hierzu unten unter D.I.3.d).

Anmeldung aufrufbare Angebot des Fanpage-Betreibers interessieren, wird oft nicht ersichtlich sein, dass sie mit dem Besuch eine Datenverarbeitung durch Facebook auslösen und z.B. durch den datr-Cookie zukünftig im Internet verfolgbar werden. Insbesondere wenn es sich um ein deutsches Fanpage Angebot handelt, werden sie daher im Zweifel auch davon ausgehen, dass das konkrete Angebot deutschem Datenschutzrecht und der Zuständigkeit deutscher Datenschutzbehörden unterliegt und sie ihre Rechte gegenüber dem Fanpage-Betreiber geltend machen müssen.[983]

Eine Untersagung des Betriebs der Fanpage bis zu einem Zeitpunkt, an dem eine datenschutzkonforme Verarbeitung der Bestands- und Nutzungsdaten der Nutzer gewährleistet ist, erweist sich damit als weit geringerer Eingriff als der hierdurch verhinderte Schaden. Es überzeugt nicht, die Unterbrechung des objektiv und subjektiv bestehenden Kausal- und Zurechnungszusammenhangs zwischen dem Betrieb der Fanpage und der später eintretenden Gefahr bzw. Verletzung mit dem Argument zu verneinen, dass es sich um eine rechtmäßige Ausübung eigener Rechte handelt.

Die privaten Fanpagebetreiber sind somit als Zweckveranlasser einzustufen und können entsprechend, mangels einer abschließenden Störerregelung im Datenschutzrecht, Adressaten einer ordnungsrechtlichen Verfügung gemäß § 38 Abs. 5 BDSG sein.[984] Ihnen kommt eine mittelbare datenschutzrechtliche Verantwortlichkeit zu, die sich allerdings rechtlich darauf beschränkt, die ihnen zuzurechnende Beförderung einer rechtswidrigen Datenverarbeitung durch einen Dritten, insbesondere Facebook, zu unterlassen.

(3) Exkurs :Mittelbare Verantwortlichkeit als zivilrechtlicher Störer

Neben der Frage der ordnungsrechtlichen Verantwortlichkeit wird in der Literatur diskutiert, inwieweit eine zivilrechtliche Störerhaftung aufgrund der mittelbaren Verletzung von Datenschutzbestimmungen durch die Fanpage-Betreiber bestehen kann.[985] Die Diskussion soll hier aufgrund des öffentlich-rechtlichen Schwerpunkts dieser Arbeit allerdings nur überblicksartig nachgezeichnet werden.

---

983 Vgl. *Weichert*, ZD 2014, 605 (609), der zudem zutreffend auf mögliche Schutzlücken hinweist, die sich ergeben könnten, wenn sich der Infrastrukturanbieter als allein verantwortliche Stelle erfolgreich der Durchsetzung des Datenschutzrechts entzöge, etwa durch einen für Verbraucher juristisch faktisch nicht erreichbaren Sitz im Ausland.

984 Im Ergebnis, wenngleich nicht der Herleitung zustimmend: *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (11 ff.).

985 Vgl. *Piltz*, K&R 2014, 80 (83 ff.); *Mantz*, ZD 2014, 62 (63 ff.); *Spindler*, GRUR Beilage 2014, 101 (108).

Die zivilrechtliche Störerhaftung zielt auf den umfassenden Schutz absoluter Rechte vor Beeinträchtigungen ab, der in den § 1004 Abs. 1 BGB in analoger Anwendung hinein gelesen wird.[986] Es ist nur konsequent, dass dieser Schutz nicht nur gegenüber einem unmittelbaren Verursacher besteht, sondern auch gegenüber mittelbaren Verursachern. Ein datenschutzrechtswidriger Umgang mit personenbezogenen Daten bedeutet regelmäßig auch eine Verletzung des allgemeinen Persönlichkeitsrechts.[987] Entsprechend überrascht es nicht, dass in der zivilrechtlichen Rechtsprechung die Möglichkeit einer mittelbaren Verantwortlichkeit wegen der Verletzung von Datenschutzbestimmungen durch eine andere verantwortliche Stelle relativ unproblematisch bejaht wurde, auch wenn dazu bisher – soweit ersichtlich – nur wenige Fälle entschieden wurden.[988]

Das *LG Potsdam* hat beispielsweise eine zivilrechtliche Störerhaftung eines Admin-C bejaht, weil auf einer von ihm mittelbar verantworteten, bei der DENIC registrierten Webseite unter wiederholtem Verstoß gegen die Vorschriften des § 4 Abs. 1 BDSG personenbezogene Daten einer Klägerin veröffentlicht wurden.[989] Indem der Beklagte sich der Betreiberin als Admin-C zur Verfügung gestellt hat, habe er „einen adäquat-kausalen Beitrag zur Verletzung des Persönlichkeitsrechts“ der Klägerin geleistet, da eine Registrierung eines Domainnamen durch einen ausländischen Antragsteller gemäß den Bestimmung der DENIC nur möglich sei, wenn eine inländische Person als Admin-C benannt werde.[990] Hiermit ging das Gericht, wenngleich ohne nähere Begründung, davon aus, dass für einen Verstoß gegen § 4 Abs. 1 BDSG eine mittelbare (zivilrechtliche) Verantwortlichkeit und entsprechend eine Pflicht zur Unterlassung und gegebenenfalls Beseitigung der Störung bestehen kann. Auch der BGH hat eine solche mittelbare Verantwortlichkeit als Mitstörer in der *Spickmich*-Entscheidung erwähnt, indes nicht näher geprüft, da es letztlich an einer rechtswidrigen Datenverarbeitung fehlte.[991]

Die vom BGH aufgestellten Hürden für die Annahme eines willentlich, adäquat kausalen Beitrags zur Begründung einer Störerhaftung sind verhältnismäßig niedrig und regelmäßig bereits durch das Betreiben einer Webseite oder die Ermöglichung des Abrufs einer Webseite

986 Ständige Rechtsprechung des BGH, vgl. statt vieler BGH, GRUR 2013, 1229 (1231), Rn. 34 m.w.N.
987 *Simitis*, in: Simitis, BDSG, § 7 Rn. 55 f. m.w.N.; *Piltz*, K&R 2014, 80 (83).
988 LG Potsdam, MMR 2013, 662 (662); BGH, NJW 2009, 2888 (2890), Rn. 15 – Spickmich; vgl. auch *Piltz*, K&R 2014, 80 (85).
989 LG Potsdam, MMR 2013, 662 (662).
990 LG Potsdam, MMR 2013, 662 (662); kritisch *Piltz*, K&R 2014, 80 (85).
991 BGH, NJW 2009, 2888 (2890), Rn. 15 – Spickmich.

erreicht.[992] Der Betrieb einer Fanpage in einem sozialen Netzwerk dürfte diese Anforderungen daher regelmäßig erfüllen.[993]

Die zivilrechtliche Störerhaftung kann mithin implizit eine Verletzung datenschutzrechtlicher Vorschriften als Rechtsverletzung voraussetzen, stellt davon abgesehen aber ein unabhängiges Regelungsregime dar. Umgekehrt wird auch die im Datenschutzrecht geregelte Haftung der für die Verarbeitung verantwortlichen Stelle durch sie nicht berührt.[994] Insbesondere kann das Bestehen einer zivilrechtlichen Verantwortlichkeit nicht herangezogen werden, um auch eine öffentlich-rechtliche Verantwortlichkeit zu begründen, da insofern – wie zuvor aufgezeigt – unterschiedliche Maßstäbe anzulegen sind.[995] *Martini* und *Fritzsche* weisen insoweit sehr zutreffend darauf hin, dass die zivilrechtliche Störerhaftung in dem „Grundgedanken der Abwehr von Besitz- und Eigentumsstörungen unter Privaten" wurzelt, insbesondere § 1004 Abs. 1 S. 1 und § 862 BGB, welche nicht geeignet sei, eine „ordnungsrechtliche Verantwortlichkeit im Subordinationsverhältnis […] zuzuordnen".[996] Die Verantwortlichkeiten können mithin parallel verlaufen, müssen dies aber nicht zwingend.

Der dogmatischen Konstruktion der zivilrechtlichen Störerhaftung durch die Rechtsprechung ist immanent, dass sie durch die Voraussetzung der Verletzung zumutbarer Pflichten begrenzt werden muss.[997] In eben diesem Punkt kann den Bedenken jener, die eine mittelbare Verantwortlichkeit für rechtswidrige Datenverarbeitungen grundsätzlich ausschließen wollen[998], Rechnung getragen werden. Der Kern der Bedenken scheint darin zu liegen, dass eine Haftung für Handlungen begründet werden soll, die außerhalb der Kontrolle des Haftenden liegen. Konkret für die Betreiber von Fanpages bei Facebook ist beispielsweise nicht klar ersichtlich und kontrollierbar, wie Facebook genau die Bestands- und Nutzungsdaten verarbeitet. Eine zu weitgehende Störerhaftung könnte daher zu Unterlassungsansprüchen führen, ohne dass die zugrundeliegende Rechtswidrigkeit der Datenverarbeitung für die Betreiber zuvor ersichtlich gewesen wäre. Sie könnten daher erheblicher Rechtsunsicherheit

992 BGH, BGHZ 191, 219 (225 f.) Rn. 21 m.w.N.
993 So auch *Piltz*, K&R 2014, 80 (83 f.).
994 *Mantz*, ZD 2014, 62 (64 f.).
995 In dieser Richtung allerdings *Spindler*, GRUR-Beilage 2014, 101 (108).
996 *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (10); vgl. auch OVG Schleswig, ZD 2014, 643 (644 f.); VG Schleswig, ZD 2014, 51 (54).
997 Vgl. hierzu bereits oben unter D.I.3.a)bb)ii).
998 OVG Schleswig, ZD 2014, 643 (644 f.); VG Schleswig, ZD 2014, 51 (54); *Piltz*, K&R 2014, 80 (84 f.); *Voigt/Alich*, NJW 2011, 3541 (3543).

und zahlreichen Klagen ausgesetzt sein, ohne sich zuvor bewusst rechtswidrig verhalten zu haben.

Dieses Problem verringert sich zum einen allerdings dadurch, dass es sich bei den in Rede stehenden Ansprüchen tatsächlich nur um solche auf Unterlassung handelt, nicht auf Schadensersatz.[999] Zum anderen müssen die Betroffenen nachweisen, dass der Betreiber der Fanpage zumutbare Prüfpflichten verletzt hat.[1000] Hierbei ist insbesondere von Bedeutung, ob für den Betreiber der Fanpage vorab erkennbar war, dass es sich bei einer Facebook Fanpage um eine in Teilen rechtswidrige Infrastruktur handelt und er daher auf ein anderes Medium hätte ausweichen sollen.[1001] Speziell in Bezug auf Facebook-Fanpages spricht indes einiges dafür – wie auch bereits zuvor im Rahmen der Stellung als Zweckveranlasser diskutiert – dass Fanpage-Betreiber durch die wiederkehrende Berichterstattung und datenschutzbehördliche Verfahren gegen Facebook jedenfalls stark sensibilisiert sein sollten.[1002] Zwar liegt bisher keine rechtskräftige Verurteilung Facebooks wegen eines Verstoßes gegen Datenschutzrecht nach dem BDSG oder TMG bei der Verarbeitung von Bestands- und Nutzungsdaten vor; allerdings wurden in mehreren Verfahren AGB-Klauseln von Facebook wegen unangemessener Benachteiligung der Nutzer in datenschutzrechtlichen Belangen für ungültig erklärt.[1003] Freilich müsste aber zivilrechtlich geklärt werden, ob in der datenschutzrechtswidrigen Verarbeitung von Bestands- und Nutzungsdaten auch eine von § 1004 Abs. 1 S. 1 BGB umfasste Verletzung des Persönlichkeitsrechts vorliegt.

Für die Belange dieser Arbeit soll insofern nur festgehalten werden, dass eine mittelbare Verantwortlichkeit von Fanpage-Betreibern im Rahmen der zivilrechtlichen Störerhaftung grundsätzlich möglich, im Einzelfall aber von der Verletzung zumutbarer Prüfpflichten und des Persönlichkeitsrechts der Betroffenen abhängig ist.[1004] Soweit eine zivilrechtliche Störerhaftung anzunehmen ist, haben Betroffene einen Anspruch auf Unterlassung der rechtswidrigen Störung, der sich im Moment faktisch wohl nur durch eine Unterlassung des Betriebs der Fanpage umsetzen ließe.

---

999 Ausführlich zur Abgrenzung: *Fritzsche*, in: Bamberger/Roth, BGB, Bd. 2, § 1004 BGB Rn. 57 ff.
1000 Vgl. allgemein zur Zumutbarkeit *Fritzsche*, in: Bamberger/Roth, BGB, Bd. 2, § 1004 BGB Rn. 65.
1001 Zur Rechtswidrigkeit von Teilen des Diensteangebots vgl. schon oben unter D.I.3.c)aa).
1002 *Petri*, ZD 2015, 103 (105); vgl. auch *Piltz*, CR 2011, 657 (663).
1003 LG Berlin, ZD 2012, 276 (277 ff.); KG Berlin, ZD 2014, 412 (414 ff.); LG Berlin, ZD 2015, 133 (134 ff.).
1004 So auch bereits *Spindler*, GRUR-Beilage 2014, 101 (108).

iii) Übertragbarkeit der Erkenntnisse auf die Rechtslage unter der DS-GVO

Die DS-GVO bietet keine neue Lösung für das Problem der mittelbaren Verantwortlichkeit, welches trotz eines sehr umfangreichen Gesetzgebungsprozesses in keinem der Entwürfe und auch nicht in der Endfassung berücksichtigt wurde. Vielmehr verharrt sie durch die Übernahme des Verantwortlichkeitsbegriffs in Art. 4 Nr. 7 DS-GVO auf dem Stand der DSRL und schafft lediglich auf Rechtsfolgenseite eine gewisse Rechtsklarheit, indem bei unklarer Verantwortlichkeit mehrerer Beteiligter gemäß Art. 26, 82 DS-GVO eine gesamtschuldnerische Haftung nach außen normiert wird.[1005]

Anders als man auf den ersten Blick denken könnte, leistet Art. 26 DS-GVO keinen Beitrag zur Klärung der mittelbaren Verantwortlichkeit und der Frage der abschließenden Regelung durch das Datenschutzrecht. Zwar könnte man *a maoire ad minus* schließen, dass wenn sogar eine vollständige gesamtschuldnerische Haftung für die speziellen datenschutzrechtlichen Pflichten, inklusive des Schadensersatzes gewollt war, die mildere Pflicht zur Beseitigung und Unterlassung nach allgemeinem Haftungsrecht erst Recht als Konsequenz gebilligt ist. Dies würde für eine abschließende Regelung innerhalb der DS-GVO sprechen, so dass zukünftig ein Rückgriff auf allgemeine ordnungsrechtliche Prinzipien nicht länger gestattet wäre. Dieses Argument geht allerdings insofern fehl, als es eine Betrachtung auf Rechtsfolgenseite darstellt, es sich bei der Frage nach dem abschließenden Charakter des Datenschutzrechts in Bezug auf die Störereigenschaft aber vornehmlich um eine des Tatbestands handelt. Eben diese wird von Art. 26 DS-GVO aber nicht adressiert, da dieser keine normative Verantwortungszuweisung als verantwortliche Stelle bei arbeitsteiligen Datenverarbeitungen auf Tatbestandsebene vornimmt.[1006] Die arbeitsteiligen Datenverarbeiter werden lediglich im Außenverhältnis schlechter gestellt und darauf verwiesen, gemäß Art. 82 Abs. 5 DS-GVO einen internen Ausgleich entsprechend ihrer tatsächlichen Verantwortlichkeit zu suchen.

Indem also der Verantwortlichkeitsbegriff unverändert bleibt, ist jedenfalls davon auszugehen, dass die oben unter i) bereits ausgeführten Feststellungen der Art. 29 Datenschutzgruppe gültig bleiben, wonach Anbieter von Online-Diensten „einen Teil der Verantwortung als für die Verarbeitung Verantwortliche“ tragen können und es entsprechend eine gleichsam

[1005] *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (16).
[1006] Vgl. *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (16); hierzu auch bereits oben unter D.I.2.b).

abgeschwächte Form der Verantwortlichkeit geben kann.[1007] Somit bleibt nur die Frage, wie diese Verantwortlichkeit zukünftig zu bestimmen ist.

Man könnte mit Blick auf Art. 58 und 83 DS-GVO zudem generell in Frage stellen, ob die ordnungsrechtliche Inanspruchnahme durch Aufsichtsbehörden überhaupt noch gegen einen anderen Adressaten als den unmittelbar datenschutzrechtlich Verantwortlichen möglich sein wird. Art. 58 und 83 DS-GVO verweisen des Öfteren ausdrücklich auf den Verantwortlichen oder Auftragsdatenverarbeiter als Adressaten. Dennoch ist aus den sogleich darzulegenden Gründen davon auszugehen, dass in dieser Hinsicht keine signifikanten Änderungen der bestehenden Rechtslage, wie sie oben analysiert wurde, eintreten werden.

Zunächst folgt aus der eben genannten Stellungnahme der Artikel-29 Datenschutzgruppe, dass im Zweifel der Begriff des Verantwortlichen „flexibel" auszulegen ist, so dass er auch mittelbare Verantwortlichkeiten umfasst.[1008] Wenngleich diese Flexibilität erhebliche Rechtsunsicherheit schaffen kann, ist sie doch nur folgerichtig mit Blick auf das grundlegende Konzept der Technologieneutralität der DS-GVO: Die Verantwortungsdiffusion, die arbeitsteilige Datenverarbeitung auszeichnet und die auch dem Problem der mittelbaren Verantwortlichkeit von Fanpage-Betreibern zugrunde liegt, ist ein technologisches Phänomen, das die ursprüngliche dichotome Aufteilung von Datenverarbeiter und Betroffenem sprengt. Es wäre sehr inkonsequent, in einem technologieneutralen Regelungskonzept strikt an einem technisch veralteten Begriff des ausschließlich unmittelbar Verantwortlichen festzuhalten, der eine arbeitsteilige, gegebenenfalls mittelbare Verantwortlichkeit konsequent ausschließt. Der Verantwortlichkeitsbegriff der DS-GVO ist damit notwendig flexibel in seiner Auslegung.

Zudem ist festzuhalten, dass gerade Art. 83 Abs. 5 DS-GVO, welcher insbesondere Bußgelder für den Verstoß gegen die grundlegenden Datenverarbeitungsvorschriften der Art. 5, 6, 7 und 9 DS-GVO normiert, so wie die bisherigen Regelungen nicht direkt einen Adressaten benennt, sondern ebenfalls erfolgsbezogen ausgerichtet ist.[1009] Dasselbe gilt für Art. 58 Abs. 2 lit. f) DS-GVO, welcher die Aufsichtsbehörden ermächtigt, eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen. Insofern besteht nach wie vor ein Spielraum im Wortlaut der Verordnung, neben dem unmittelbar Verantwortlichen auch einen anderen Störer zur Verantwortung zu ziehen.

[1007] Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 14.
[1008] Art. 29 DatSchGruppe, Stellungnahme 2/2010, WP 171, S. 14.
[1009] Zur bisherigen Rechtslage *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (9 ff.).

Zuletzt lässt die DS-GVO nicht erkennen, dass eine Veränderung an dem oben analysierten Verhältnis zwischen dem umfassend harmonisierten Datenschutzrecht und dem allgemeinen Haftungsrecht beabsichtigt war. Dennoch wird sich – im Vergleich zur bisherigen Rechtslage – ein Rückgriff auf nationale ordnungsrechtliche Störerkategorien aufgrund der unterschiedlichen Normebenen deutlich schwieriger gestalten. Eine Verfügung gemäß Art. 58 Abs. 2 lit. f) oder Art. 83 Abs. 5 DS-GVO kann aufgrund der unterschiedlichen Normebenen nicht direkt mit der im deutschen Ordnungsrecht verhafteten Figur des Zweckveranlassers legitimiert werden. Dies ist angesichts der gebotenen weiten Auslegung des Verantwortlichkeitsbegriffs der DS-GVO indes auch nicht erforderlich. Daher ist zu empfehlen, die oben im Rahmen der Frage nach der Stellung als Zweckveranlasser angestellten Überlegungen zur dogmatischen Strukturierung und Fallgruppenbildung zu verwenden, um den weiten Verantwortlichkeitsbegriff der DS-GVO besser zu strukturieren.

Für die mittelbare Verantwortlichkeit von Fanpage-Betreibern insbesondere bei Facebook bedeutet die neue Rechtslage somit keine materiell-rechtlichen Änderungen, sondern allenfalls eine neue, vereinfachte dogmatische Konstruktion über die unmittelbare Anwendbarkeit eines weiter gefassten Verantwortlichkeitsbegriffs.

dd) Zulässigkeit von Fanpages der öffentlichen Hand

Unabhängig von der Frage nach der mittelbaren Verantwortlichkeit privater Fanpagebetreiber stellt sich die Frage nach der Zulässigkeit der Nutzung von Facebook Fanpages durch die öffentliche Hand.

Diese bedient sich mittlerweile verhältnismäßig häufig sozialer Netzwerke, vor allem zu Zwecken des Marketings und der Kommunikation.[1010] Durch die enorme Verbreitung sozialer Netzwerke erhoffen sich staatliche Akteure, die Reichweite ihrer Kommunikationsangebote zu erhöhen. Entsprechend gibt es für viele öffentliche Stellen mittlerweile „Fanpages“, auf denen diese in Kontakt mit den Bürgern treten. Als Beispiele seien hier genannt: Die Facebookseiten der deutschen Bundesregierung[1011], zahlreicher Polizeibehörden[1012], der Bundeswehr[1013] und

[1010] Für einen Überblick vgl. *Gerhold*, ZIS 2015, 156 (156 f., 163 f.); *Caspar*, ZD 2015, 12 (12 ff.); *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (125); *Weis*, Fanpages der öffentlichen Hand, in: Hill/Wagner/Martini (Hrsg.), Facebook, Google & Co, S. 63 f.

[1011] https://de-de.facebook.com/Bundesregierung.

[1012] Vgl. z.B. https://de-de.facebook.com/polizeihamburg; https://de-de.facebook.com/PolizeiBerlin; https://de-de.facebook.com/ppmuenchen; https://de-de.facebook.com/pages/Polizei-NRW/359721787378033; ausführlich hierzu: *Gerhold*, ZIS 2015, 156 (156 f., 163 ff.); *Weichert*, JBÖS 2012/2013, 379 (381 ff.).

[1013] https://de-de.facebook.com/Bundeswehr.

verschiedener Landesparlamente[1014], sowie des Bundestags[1015]. Viele Städte und Kommunen sind ebenfalls bereits mit eigenen Seiten bei Facebook vertreten.[1016] Ähnliche Seiten finden sich auch bei Google Plus[1017], wobei eine stichprobenartige Untersuchung darauf hindeutet, dass die Präsenz bei Facebook insgesamt deutlich ausgeprägter ist.[1018]

Die Nutzung derartiger Seiten durch öffentliche Stellen stellt ein Dilemma dar. Einerseits ist es durchaus Aufgabe des (transparenten) Staates, mit seinen Bürgern auf angemessene und zeitgemäße Weise in Kontakt zu treten.[1019] Eine Verweigerung moderner Kommunikationsmethoden schränkt die Kontaktmöglichkeiten erheblich ein und führt somit zur Abschottung öffentlicher Stellen. Gerade Facebook hat sich mit seiner enormen Verbreitung insoweit zu einer wichtigen Kommunikationsplattform entwickelt; es gibt mittlerweile sogar Nutzer, die ihre Informationen aus dem Internet fast nur noch via Facebook beziehen.[1020]

Andererseits stellt die durch den Betrieb von Fanpages kausal verursachte und geförderte, rechtswidrige Datenverarbeitung durch Facebook ein besonderes Problem für öffentliche Stellen dar, welche gemäß Art. 20 Abs. 3 GG an Recht und Gesetz gebunden sind. Es erscheint schon auf den ersten Blick wenig überzeugend, der öffentlichen Hand, die selbst an Recht und Gesetz gebunden ist, zuzugestehen, zur Erfüllung eigener Aufgaben auf rechtswidrig handelnde Dritte zurückzugreifen und von deren Verhalten zu profitieren. Dieser Eindruck bestätigt sich in einer tieferen Analyse.

Wie im vorigen Abschnitt bereits gezeigt wurde, besteht eine mittelbare Verantwortlichkeit privater Fanpage-Betreiber für die rechtswidrige Datenverarbeitung durch Facebook. Für die öffentliche Hand können insoweit keine großzügigeren Maßstäbe gelten als für private Akteure, zumal sich staatliche Akteure gerade nicht auf eigene Grundrechte zur Rechtfertigung ihres

---

[1014] Vgl. z.B https://de-de.facebook.com/pages/Bayerischer-Landtag/210015922345399; https://de-de.facebook.com/pages/Hessischer-Landtag/140747145967416

[1015] https://de-de.facebook.com/pages/Deutscher-Bundestag/386473598058533.

[1016] Vgl. z.B. https://de-de.facebook.com/Hamburg; https://de-de.facebook.com/wuerzburg; https://de-de.facebook.com/Hauptstadtportal; https://www.facebook.com/tuebingen/timeline?ref=page_internal.

[1017] Vgl. z.B. https://plus.google.com/+bundeswirtschaftsministerium/posts; https://plus.google.com/s/Bundesregierung; https://plus.google.com/s/Bundestag; https://plus.google.com/+BerlinTourismus/posts; für die Polizei in Sachsen: https://plus.google.com/101688436473687232481/posts.

[1018] Zur insgesamt deutlich größeren Verbreitung von Facebook vgl. bereits oben unter B.I.

[1019] *Gerhold*, ZIS 2015, 156 (164); *Martini/Fritzsche*, VerwArch (104) 2013, 449 (468 f.); *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (125 f.).

[1020] *Reuters Institute*, http://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital-News-Report-2016.pdf, S. 8 f.; *Gerhold*, ZIS 2015, 156 (164).

Tuns berufen können. Freilich ist umstritten, ob staatliche Akteure, insbesondere solche aus der Verwaltung, als Störer eingestuft und entsprechend Adressaten ordnungsrechtlicher Verfügungen sein können.[1021] Diese Frage ist indes bei der Bestimmung der Zulässigkeit von Fanpages der öffentlichen Hand von nachrangiger Bedeutung, da sie primär die formelle Polizeipflichtigkeit betrifft. Dass staatliche Akteure einer materiellen Polizeipflichtigkeit unterliegen, ist mit Blick auf ihre Bindung an Recht und Gesetz allgemein anerkannt.[1022] Ihre formelle Einordnung als Störer erübrigt sich somit, wenn ein Verhalten rechtswidrige Folgen hat, da sie bereits qua ihrer Bindung an Recht und Gesetz unmittelbar verpflichtet sind, dieses Verhalten zu unterlassen.[1023]

Es ist allgemein anerkannt, dass die öffentlichen deutschen Stellen bei ihrem Handeln bisher der Geltung deutschen Datenschutzrechts unterliegen. Unabhängig davon, ob man auf Facebook insgesamt die Regelungen des BDSG und des TMG für anwendbar hält, sind diese daher jedenfalls von der öffentlichen Hand bei dem Betrieb von Fanpages zu beachten.[1024] Dasselbe gilt zukünftig für die Regelungen der DS-GVO, soweit diese auf öffentliche Stellen Anwendung finden bzw. selbstverständlich auch für die Regelungen des BDSG n.F. gemäß Art. 1 DSAnpUG-EU.

Befürworter einer Zulässigkeit des Betriebs einer Fanpage durch die öffentliche Hand – trotz der mutmaßlich rechtswidrigen Datenverarbeitung durch Facebook – verweisen darauf, dass ein Verzicht auf die Möglichkeiten des Einsatzes von Social Media Angeboten eine unverhältnismäßige Einschränkung der Kommunikationsmöglichkeiten der öffentlichen Hand darstelle.[1025] Zudem erweise sich der hiermit erfolgende mittelbar-faktische Eingriff in die informationelle Selbstbestimmung von Nutzern dieser Fanpages als vergleichsweise mild, so dass er verhältnismäßig sei.[1026]

Diese Argumentation verfehlt indes das Problem. Die öffentliche Hand darf sich nicht an Rechtsbrüchen beteiligen, nur weil es praktisch, „für die behördliche Aufgabenerfüllung von großem Nutzen“[1027] oder kostensparend ist. Eine Ermächtigungsgrundlage kann nicht zu

---

[1021] Instruktiv: *Schenke*, POR, § 4 Rn. 233 f.; *Denninger*, in: Handbuch des Polizeirechts, D Rn. 95 ff. m.w.N.
[1022] *Schenke*, POR, § 4 Rn. 233; *Denninger*, in: Handbuch des Polizeirechts, D Rn. 96 f. m.w.N.
[1023] *Caspar*, ZD 2015, 12 (15).
[1024] OVG Schleswig, ZD 2014, 643 (643 f.); VG Schleswig, ZD 2014, 51 (52 f.); *Caspar*, ZD 2015, 12 (14); *Gerhold*, ZIS 2015, 156 (159); *Schulz/Hoffmann*, in: PdK, Band L 16 Bund, Rn. 72; *Martini/Fritzsche*, VerwArch (104) 2013, 449 (461 f.).
[1025] *Gerhold*, ZIS 2015, 156 (164).
[1026] *Gerhold*, ZIS 2015, 156 (163 f.).
[1027] So *Gerhold*, ZIS 2015, 156 (164).

rechtswidrigem Verhalten ermächtigen, da dies einen Widerspruch in der Einheit der Rechtsordnung darstellen würde. Vielmehr müsste sie eine explizite Ausnahme zu geltenden Datenschutzvorschriften enthalten. Eine entsprechende Regelung existiert indes nicht. Dies gilt umso mehr, wenn das in Frage stehende Verhalten grundrechtsrelevant ist, wie vorliegend für die informationelle Selbstbestimmung der Nutzer.[1028]

Daher ist der Einsatz von Facebook Fanpages durch die öffentliche Hand unter den gegenwärtigen, oben beschriebenen Bedingungen der Verarbeitung von Bestands- und Nutzungsdaten unzulässig.[1029] Selbst wenn man eine mittelbare Verantwortlichkeit für die rechtswidrige Datenverarbeitung durch Facebook ablehnt – quod non –, so widerspricht es der verfassungsrechtlichen Verantwortung und Bindung staatlicher Stellen, derartige Fanpages zu betreiben.[1030] Keinesfalls dürfen Angebote exklusiv über soziale Medien nutzbar sein, die Bürger also faktisch gezwungen werden, diese Infrastruktur zu nutzen.[1031]

ee) Zwischenergebnis: Datenschutzrechtliche Verantwortlichkeit der Betreiber von „Fanpages“

Der Betrieb von Facebook Fanpages ist zum jetzigen Zeitpunkt mit erheblichen Datenschutzverstößen seitens Facebooks verbunden. Mit dem Aufruf der Fanpage werden automatisch Cookies übertragen, die eine Verfolgung des Nutzerverhaltens sowohl auf der Fanpage, als auch auf anderen Internetseiten mit Social PlugIns und damit eine erhebliche Reichweitenanalyse ermöglichen. Die anfallenden Bestands- und Nutzungsdaten werden entgegen der Regelung des § 15 Abs. 3 TMG durch Facebook mit personenbezogenen Daten über den Träger des Pseudonyms verbunden und den Betreibern von Fanpages in Form der Statistik „Facebook Insights“ zur Verfügung gestellt. Diese Funktion ist für die Fanpage-Betreiber nicht abbestellbar und damit zwingend mit dem Betrieb der Fanpage verbunden. Die Daten in der Statistik sind zwar anonymisiert; sie bieten dennoch einen erheblichen wirtschaftlichen Vorteil für die Betreiber, die hiermit ihre Fanpage besser auf ihre Zielgruppe ausrichten können.

Mangels eines hinreichenden Einflusses auf die Zwecke und Mittel dieser Datenverarbeitung sind die Fanpage-Betreiber dennoch nicht als unmittelbar verantwortliche Stelle einzustufen.

1028 *Caspar*, ZD 2015, 12 (15).

1029 Bayrischer Landesdatenschutzbeauftragter, https://www.datenschutz-bayern.de/technik/orient/oh_fanpages.pdf, S. 19; vgl. auch *Martini/Fritzsche*, VerwArch (104) 2013, 449 (468), deren Analyse sich zwar auf Social PlugIns bezieht, im Kern aber übertragbar ist.

1030 *Caspar*, ZD 2015, 12 (15); *Weichert*, JBÖS 2012/2013, 379 (381 ff.).

1031 *Martini/Fritzsche*, VerwArch (104) 2013, 449 (465 f.).

Die bloße Initiierung der Datenverarbeitung genügt als qualifizierende Handlung nicht aus und würde das Merkmal der verantwortlichen Stelle bis zur Unkenntlichkeit verwässern. Auch die Annahme einer Auftragsdatenverarbeitung gemäß § 11 BDSG bzw. Art. 28 DS-GVO zwischen dem Fanpage-Betreiber und Facebook wäre eine reine Fiktion, da gegenüber Facebook effektiv keinerlei Kontroll- und Weisungsbefugnisse bestehen.

Die Betreiber von Fanpages sind aber mittelbar verantwortlich für die von Facebook vorgenommene Datenverarbeitung. Zivilrechtlich können gegen sie Unterlassungsansprüche aus der Störerhaftung gemäß § 1004 BGB analog begründet sein. Öffentlich-rechtlich sind sie nach bisheriger Rechtslage für die Verwendung der Bestands- und Nutzungsdaten durch Facebook zu Zwecken der Profilerstellung als Zweckveranlasser einzustufen und können daher auch Adressaten einer ordnungsrechtlichen Verfügung gemäß § 38 Abs. 5 BDSG sein, da das Datenschutzrecht insoweit nicht als abschließende Regelung einzustufen ist. Dieselbe Verantwortlichkeit wird auch unter der DS-GVO bestehen und u.a. Verfügungen nach Art. 58 Abs. 2 lit. f) DS-GVO ermöglichen.

Nach den gleichen Maßstäben ist eine Nutzung von Facebook-Fanpages durch die öffentliche Hand zum gegenwärtigen Zeitpunkt unzulässig. Insbesondere aufgrund der Gesetzesbindung der Verwaltung darf diese nicht mittelbar von einer Rechtsverletzung durch Facebook profitieren und die informationelle Selbstbestimmung der Nutzer gefährden.

d) Verantwortlichkeit der Verwender von Social PlugIns

Social PlugIns wurden bereits im Zusammenhang mit Tracking-Methoden sozialer Netzwerke oben unter B.II.2.b)aa) angesprochen. Im Folgenden soll es darum gehen, inwiefern die Webseitenbetreiber, die die Social PlugIns auf ihren Webseiten integrieren, für die daraus resultierende Datenverarbeitung verantwortlich sind. Hierfür soll zunächst vertieft dargelegt werden, welche Funktionen Social PlugIns ermöglichen und welchen Nutzen sie entsprechend den Webseitenbetreibern bieten.

Social PlugIns ermöglichen es Nutzern sozialer Netzwerke unter anderem, die auf der Webseite veröffentlichten Inhalte direkt in ihrem sozialen Netzwerkprofil zu teilen, indem sie auf die Schaltfläche klicken. Hierdurch wird eine Meldung in dem Nutzerprofil erstellt, wonach dem Nutzer diese bestimmte Webseite „gefällt“ bzw. er den Inhalten auf dieser Webseite „folgt“.

Die Kontakte der Nutzer können hiervon Kenntnis nehmen, wodurch sich die Reichweite des Webseitenangebots deutlich erhöhen kann.[1032]

In vielen Fällen ist es zudem möglich, sich auf einer Webseite zur Nutzung von Kommentierungsfunktionen und Ähnlichem nicht mit einem gesonderten Account der Webseite, sondern mit seinem sozialen Netzwerk-Account einzuloggen. Dies reduziert für Nutzer die Anzahl der von ihnen zu verwaltenden Accounts und ermuntert sie daher gegebenenfalls, sich auf mehr Webseiten anzumelden, wovon sowohl deren Betreiber, als auch die Anbieter sozialer Netzwerke profitieren, die hierdurch noch mehr Daten erhalten.

Social PlugIns sind zu weitgehendem Tracking der Nutzer geeignet, da die Anbieter sozialer Netzwerke durch mit den PlugIns kommunizierende Cookies über die Aktivitäten der Nutzer auf der jeweiligen Seite informiert werden können. Wie bereits oben dargelegt, sendet beispielsweise der datr-Cookie, der bei jedem Besuch der Domain facebook.com auf dem Endgerät abgelegt wird und bis zu zwei Jahre gültig bleibt, bei jedem nachfolgenden Besuch einer Webseite mit einem Like-Button Informationen an Facebook.[1033] Zudem erhält Facebook die IP-Adresse des Nutzers, je nach technischer Einbindung des Like-Buttons sogar unabhängig davon, ob dieser tatsächlich angeklickt wurde oder nicht, hierzu sogleich mehr.[1034] Die derart gewonnenen Informationen können, wie alle anderen gesammelten Informationen, von den Anbietern sozialer Netzwerke genutzt werden, um ausführliche Profile der Nutzer zu erstellen und hierdurch Werbung gezielter zu vermarkten, worauf beispielsweise Facebook auch ausdrücklich in seinen Datenrichtlinien hinweist.[1035]

Wie Fanpage-Betreiber erhalten die Verwender des Facebook Like-Buttons zudem Zugriff auf die anonymisierte Statistik Facebook Insights.[1036] Die durch das Social PlugIn ausgelöste

---

[1032] *Ernst*, NJOZ 2010, 1917 (1917 f.); *Maisch*, Informationelle Selbstbestimmung, S. 208 ff.; vgl. auch *Lichtnecker*, GRUR 2013, 135 (136); *Hoffmann-Riem*, Innovation und Recht, S. 625 f.

[1033] *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 89 f.; *Karg/Thomsen*, DuD 2012, 729 (730 f.); vgl. zum datr-Cookie auch schon oben unter B.II.2.b)aa).

[1034] ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 7 f.; *Voigt/Alich*, NJW 2011, 3541 (3541 f.); *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1, Rn. 47.

[1035] „Wir sammeln Informationen, wenn du Webseiten und Apps Dritter besuchst, die unsere Dienste nutzen (z. B. wenn sie unsere „Gefällt mir"-Schaltfläche oder die Facebook-Anmeldung anbieten oder unsere Bewertungs- und Werbedienste nutzen). Dazu zählen auch Informationen über die von dir besuchten Webseiten und Apps und über deine Nutzung unserer Dienste auf solchen Webseiten und Apps sowie Informationen, die der Entwickler oder Herausgeber der App oder Webseite dir bzw. uns zur Verfügung stellt.", https://www.facebook.com/privacy/explanation (Stand 29. September 2016); kritisch hierzu *Ernst*, NJOZ 2010, 1917 (1917 f.).

[1036] *Karg/Thomsen*, DuD 2012, 729 (731); *Maisch*, Informationelle Selbstbestimmung, S. 209; ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 12; vgl. auch oben unter D.I.3.c)aa).

Datenverarbeitung durch Facebook ist weitgehend vergleichbar mit derjenigen, die infolge des Aufrufs von Fanpages geschieht. Daher stellt sich ebenso wie bei den Fanpage-Betreibern die Frage nach der datenschutzrechtlichen Verantwortlichkeit. Vergleichbar zu den Betreibern von Fanpages hängt insbesondere eine mittelbare Verantwortlichkeit der Social PlugIn Verwender für die Datenverarbeitung durch Facebook davon ab, ob sie durch die Art der Einbindung des Social PlugIns eine automatische Übermittlung der Daten zulassen und ob die anschließend erfolgende Verarbeitung durch Facebook rechtmäßig ist. Denn sowohl die zivilrechtliche Störerhaftung als auch die mittelbare Verantwortlichkeit als Zweckveranlasser beruhen darauf, dass ein rechtswidriges Verhalten eines Dritten zugerechnet wird. Wenn das Verhalten des Dritten rechtlich nicht zu beanstanden ist, dann entfällt auch der Zurechnungszusammenhang.

Es existieren unterschiedliche technische Möglichkeiten, Social PlugIns auf Webseiten einzubinden. Die Unterscheidung hat erhebliche Auswirkungen auf die Beurteilung der datenschutzrechtlichen Verantwortlichkeit sowie Rechtmäßigkeit der Datenverarbeitung, wie sogleich deutlich werden wird. Vereinfachend seien die Möglichkeiten hier kategorisiert in eine direkt-sendende Variante und eine datenschutzfreundlichere Variante in Form der sogenannten „2-Klick Lösung".

Wählt der Anbieter die direkt-sendende Variante, werden die oben beschriebenen Daten über die Cookies unmittelbar beim Aufruf der Seite an den Anbieter des sozialen Netzwerks gesendet, auch wenn der Nutzer nicht auf den Social PlugIn Button geklickt hat. Der Nutzer kann somit nicht verhindern, dass sein Besuch auf der Webseite von dem Anbieter des sozialen Netzwerks registriert wird, sofern sich der entsprechende Cookie – gegebenenfalls ohne sein Wissen – auf seinem Endgerät befindet.[1037] Bei der „2-Klick Lösung" sind die Social PlugIn Buttons dagegen nicht sofort mit Aufruf der Seite „aktiv". Vielmehr muss der Nutzer zunächst bewusst auf diese klicken und gegebenenfalls mit einem zweiten Klick sein Einverständnis in die Datenübermittlung erklären, bevor diese erfolgt.[1038] Bis März 2015 wurden grundsätzlich beide Varianten von Facebook zur Integration angeboten. Im Laufe des März 2015 wurden aber von den bis dahin vier verfügbaren Integrationsoptionen drei deaktiviert. Die verbliebene

[1037] *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 99.

[1038] *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 99; *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG, Rn. 12; *Moos*, in: Taeger/Gabel, § 13 TMG Rn. 21; *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 145; *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1, Rn. 49; vgl. auch: http://www.heise.de/ct/ausgabe/2014-26-Social-Media-Buttons-datenschutzkonform-nutzen-2463330.html.

Integrationsoption führt zu einer Sofortübertragung der genannten Daten.[1039] Auch ohne dass Facebook eine mit der „2-Klick Lösung" vergleichbare datenschutzfreundliche Möglichkeit zur Integration anbietet, kann eine solche aber immer noch über Drittanbieter erreicht werden, welche z.B. den Like-Button technisch modifizieren und so eine Form der Integration in Webseiten ermöglichen, bei der Nutzerdaten nicht sofort übertragen werden.[1040]

Entscheidend ist für die rechtliche Beurteilung, vergleichbar zu den Fanpage-Betreibern, ob bereits die Initiierung der Datenübertragung an den Anbieter des sozialen Netzwerks eine relevante Form der Datenverarbeitung darstellt. Zudem ist zu untersuchen, ob aus Gegenleistungen des sozialen Netzwerkanbieters wie der detaillierten „Facebook-Insights"-Statistik datenschutzrechtliche Konsequenzen resultieren.

Eine unmittelbare datenschutzrechtliche Verantwortlichkeit ist aus denselben Gründen abzulehnen wie sie bereits für die Fanpage-Betreiber unter D.I.3.c)bb) ausführlich diskutiert wurden.[1041] Die Social PlugIn Verwender haben ebenso wie die Fanpage-Betreiber keinen Einfluss auf die Zwecke und Mittel der Datenverarbeitung und nehmen sie diese auch nicht selbst vor. Die bloße Initiierung der Datenverarbeitung und die damit verbundene Entscheidung über das „Ob" der Datenverarbeitung genügt noch nicht, um eine hinreichende Kontrolle über die Datenverarbeitung anzunehmen, da es bei einer derartigen Verwässerung des Begriffs zu unhaltbaren Abgrenzungsproblemen käme. Auch wirtschaftlich ist die erfolgende Datenverarbeitung nicht in einem Maße mit ihrer eigenen Tätigkeit verbunden, dass hier ein

---

1039 So *Van Alsenoy u.a.*, Https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 99. Interessanterweise zeigt eine Statistik zur Einbettung von Like-Buttons seit April 2015 einen deutlichen Einbruch der Verwendung des Like-Buttons auf den meistbesuchten Webseiten, wobei ein Zusammenhang allerdings nur vermutet werden kann, vgl. http://trends.builtwith.com/widgets/Facebook-Like. In derselben Grafik spiegelt sich dieser Einbruch in der Verbreitung des Like-Buttons im gesamten Internet indes nicht wider, so dass die Zuverlässigkeit der Quelle in Frage gestellt werden muss.

1040 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 99; http://www.heise.de/ct/ausgabe/2014-26-Social-Media-Buttons-datenschutzkonform-nutzen-2463330.html.

1041 So auch *Piltz*, CR 2011, 657 (662); *Maisch*, Informationelle Selbstbestimmung, S. 213 ff.; *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG, Rn. 12 und *Moos*, in: Taeger/Gabel, § 11 TMG, Rn. 29 ff., die aber dennoch Informationspflichten gemäß § 13 Abs. 1 TMG bejahen, vgl. *Moos*, in: Taeger/Gabel, § 13 TMG, Rn. 33; a.A. LG Düsseldorf, ZD 2016, 231 (232 f.), Rn. 48 ff.; *Ernst*, NJOZ 2010, 1917 (1918); ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 17 f.; *Moser-Knierim*, ZD 2013, 263 (264), die eine Funktionsübertragung von Facebook auf den Social PlugIn Verwender annimmt und damit zu dessen voller datenschutzrechtlicher Verantwortlichkeit gelangt (vgl. zum Begriff der Funktionsübertragung in Abgrenzung zur Auftragsdatenverarbeitung *Spindler/Nink*, in: Spindler/Schuster, § 11 BDSG Rn. 13 und *Gola/Schomerus*, § 11 Rn. 9). Dies überzeugt indes nicht, da die Verwender von Social PlugIns nicht von Facebook beauftragt werden, in eigener Verantwortung Daten über das Social PlugIn zur Förderung des eigenen Angebots zu erheben und zu verarbeiten. Die konkrete Datenverarbeitung wird vielmehr ausschließlich durch Facebook kontrolliert, ohne dass den Social PlugIn Verwendern irgendwelche Entscheidungsbefugnisse zukommen, außer diese durch eine entsprechende technische Einbindung vollständig zu unterbinden, vgl. auch *Martini/Fritzsche*, NVwZ-Extra (21) 2015, 1 (6 f.).

untrennbarer Zusammenhang bestünde.[1042] Facebook gibt zudem die Bedingungen des Einsatzes des Like-Buttons unverhandelbar vor und unterliegt keiner Weisungsbefugnis durch die Verwender, so dass die Annahme einer Auftragsdatenverarbeitung wiederum eine bloße Fiktion darstellen würde.[1043]

Für die aus dem Einsatz von Social PlugIns resultierende Datenverarbeitung kann in der Regel nicht davon ausgegangen werden, dass diese vollständig durch einen gesetzlichen Erlaubnistatbestand gedeckt ist. Insbesondere die damit von Facebook vorgenommene Reichweitenanalyse ist zur Erbringung der Dienste weder erforderlich, noch ist in einer Interessenabwägung davon auszugehen, dass das Interesse der Nutzer an informationeller Selbstbestimmung hinter Facebooks wirtschaftlichen Interessen zurücktritt.[1044] Soweit allerdings die 2-Klick-Lösung oder vergleichbare Technologien verwendet werden, inklusive einer Aufklärung über die Folgen einer Aktivierung, spricht viel dafür, von einer Einwilligung des Nutzers in die durch Facebook erfolgende Datenverarbeitung auszugehen, wodurch diese rechtmäßig würde.[1045]

Wenn die Datenübermittlung automatisch mit Aufruf der Webseite geschieht, ohne dass die Nutzer zuerst das Social PlugIn durch einen Klick aktivieren, liegt dagegen keine bewusste Einwilligung der Nutzer vor.[1046] In dieser Konstellation können die Nutzer überhaupt erst nach Aufruf der Webseite feststellen, ob diese ein Social PlugIn verwendet. In diesem Moment wäre

---

[1042] a.A. *Martini/Fritzsche*, VerwArch (104) 2013, 449 (463), die eine unmittelbare Verantwortlichkeit aufgrund einer Partizipation an Reichweitenanalysen und Nutzungsstatistiken bejahen: Jedenfalls eine öffentliche Stelle, die Social PlugIns mit diesem Ziel verwende, sei „in dieser Dreieckskonstellation nicht anders zu behandeln, als wenn sie die Daten selbst verarbeiten würde."; ebenfalls a.A. *Ernst*, NJOW 2010, 1917 (1918); *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner, S. 428.

[1043] *Ernst*, NJOW 2010, 1917 (1918); vgl. auch *Piltz*, CR 2011, 657 (662); *Schröder/Hawxwell*, Verletzung datenschutzrechtlicher Bestimmungen, in: Wissenschaftlicher Dienst des BT, S. 8 f.

[1044] *Martini/Fritzsche*, VerwArch (104) 2013, 449 (457 ff.).

[1045] So auch *Moos*, in: Taeger/Gabel, § 13 TMG Rn. 21, 33; *Martini/Fritzsche*, VerwArch (104) 2013, 449 (467); vgl. auch Belgian Privacy Commission, Recommendation no. 04/2015 of 13.05.2015, S. 26 f.; Man könnte freilich in Frage stellen, ob der Nutzer den Umfang der damit verbundenen Datenverarbeitung richtig einschätzen kann und damit hinreichend informiert entscheidet, vgl. *Moser-Knierim*, ZD 2013, 263 (265). Letztendlich wird man dies aber bejahen müssen, da gerade dem mündigen Verbraucher und Bürger auch ein gewisses Maß an Eigenverantwortlichkeit zugeschrieben werden muss. Wer sich entscheidet, bewusst ein Social PlugIn zu aktivieren, trotz eines Hinweises auf hieraus resultierende Datenverarbeitung Facebooks, dem kann zugemutet werden, sich hiermit näher auseinanderzusetzen. Anders als bei dem bloßen Besuch einer Fanpage wird hier bewusst auf eine von Facebook zur Verfügung gestellte Funktion zurückgegriffen, die mit dem eigentlichen Inhalt der Webseite erkennbar nichts zu tun hat. Dem Nutzer wird somit unmittelbar klar gemacht, dass er hier eine Handlung gegenüber Facebook vornimmt.

[1046] So auch *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1, Rn. 49; LG Düsseldorf, ZD 2016, 231 (232 f.), Rn. 48 ff.

es für eine Verhinderung der Datenübermittlung aber bereits zu spät. Mangels Kenntnis von der Datenübertragung können sie nicht *ex ante* in diese einwilligen und sie auch nicht verhindern.

Anders als Betreiber von Fanpages haben Social PlugIn Verwender auch eine umfassende Kontrolle über die Initiierung der automatischen Datenverarbeitung durch Facebook, da sie diese durch die konkrete technische Einbindung des Like-Buttons beeinflussen und sogar ganz verhindern können.[1047] In umgekehrter Betrachtung nehmen sie diese Datenverarbeitung bewusst in Kauf, wenn sie auf die Verwendung von technisch verfügbaren Möglichkeiten wie der 2-Klick-Lösung verzichten. Sie profitieren von der Vergrößerung der Reichweite, die durch die gezielte Anzeige von Nutzeraktivitäten auf ihrer Seite bei den Facebook-Freunden des Besuchers bewirkt wird. Dieser Vorteil beruht wiederum auf einer jedenfalls teilweise rechtswidrigen Nutzerprofilanalyse durch Facebook. Zudem erhalten auch sie Zugriff auf Facebook Insights, dessen Erkenntnisse ohne eine Einwilligung oder Widerspruchsrechte der Nutzer unter Verstoß gegen §§ 13 Abs. 1, 15 Abs. 3 TMG bzw. Art. 6, 12 ff. und 19 DS-GVO gesammelt und zusammengestellt werden.[1048] Sie sind daher als Zweckveranlasser einzustufen und somit mögliche Adressaten ordnungsrechtlicher Verfügungen gemäß § 38 Abs. 5 BDSG bzw. zukünftig Art. 58 DS-GVO als mittelbar Verantwortliche.[1049]

Verwender von Social PlugIns sind somit ebenso wenig wie die Betreiber von Fanpages unmittelbar verantwortliche Stellen für die durch Facebook erfolgende Datenverarbeitung. Sie sind aber mittelbar für diese verantwortlich, sofern sie durch die Art der Einbindung des Social PlugIns eine automatische Datenübermittlung ermöglichen. Sie sind in solchen Konstellationen Adressaten von zivilrechtlichen und öffentlich-rechtlichen Unterlassungspflichten und können entsprechend als Störer zur Verantwortung gezogen werden, wenn sie diesen Pflichten nicht nachkommen.

e) Verantwortlichkeit von Anbietern externer Inhalte: Apps, Spieleentwickler etc.

Facebook ermöglicht es Dritten, Angebote in das soziale Netzwerk einzubinden und dessen Nutzern auf diese Weise zur Verfügung zu stellen. Hierbei handelt es sich häufig um (Browser-)Spiele wie das zu einiger Bekanntheit und Verbreitung gelangte „FarmVille“, sowie um

[1047] Vgl. auch *Martini/Fritzsche*, VerwArch (104) 2013, 449 (467); *Schröder/Hawxwell*, Verletzung datenschutzrechtlicher Bestimmungen, in: Wissenschaftlicher Dienst des BT, S. 8; LG Düsseldorf, ZD 2016, 231 (233 f.), Rn. 49 ff.

[1048] *Martini/Fritzsche*, VerwArch (104) 2013, 449 (459 f., 464 f.); *Karg/Thomson*, DuD 2012, 729 (731); ULD, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, S. 12 ff.

[1049] Hierzu ausführlich, insbesondere zur nicht-abschließenden Regelung durch das Datenschutzrecht, oben unter D.I.3.c)cc)i); teilweise a.A. *Martini/Fritzsche*, VerwArch (104) 2013, 449 (462 ff.) und *Ernst*, NJOZ 2010, 1917 (1918), die eine unmittelbare datenschutzrechtliche Verantwortlichkeit bejahen.

Umfragen, Horoskope oder andere Apps. Insbesondere Spiele sind häufig mit sogenannten Mikrotransaktionen verbunden: Während die Spiele selbst grundsätzlich kostenlos nutzbar sind, ist es möglich, durch Überweisung kleiner Geldbeträge zusätzliche Gegenstände oder Optionen zu erhalten, die ansonsten überhaupt nicht oder nur nach längerem Warten zur Verfügung stehen würden. Während die Beträge für sich genommen häufig vernachlässigbar gering sind, generieren sie in der Summe erhebliche Mengen an Einnahmen, von denen die Anbieter des sozialen Netzwerks in der Regel einen bestimmten Anteil in Form von Gebühren erhalten. Im Fall Facebooks wurde mit derartigen Gebühren im Jahr 2013 ein Umsatz von 886 Millionen US-Dollar generiert, was damals noch einen Anteil von 11,26% am Gesamtumsatz von 7,87 Milliarden US-Dollar ausmachte.[1050] Im Jahr 2014 lag dieser Umsatz bereits bei 974 Millionen US-Dollar, was allerdings nur noch einen Anteil von 7,81% am Gesamtumsatz von 12,47 Milliarden US-Dollar bedeutete.[1051] Im Jahr 2015 verringerte sich der Anteil am Gesamtumsatz von nunmehr 17,93 Milliarden US-Dollar auf nur noch 4,74 %, wenngleich die Einnahmen durch vergleichbare Gebühren nominal relativ stabil bei 849 Millionen US-Dollar blieben.[1052]

Von Bedeutung für diese Arbeit ist, dass die Anbieter solcher Apps regelmäßig Zugriff auf insbesondere Profildaten derjenigen Nutzern erhalten, die diese Apps nutzen. Darüber hinaus kann ihnen auch Zugriff auf Profildaten der Kontakte dieser Nutzer gewährt werden, ohne dass diese Kontakte hiervon erfahren.[1053] Ob die Übermittlung der Daten durch Facebook an derartige Anbieter überhaupt datenschutzrechtlich zulässig ist, wird kritisch gesehen und wurde beispielsweise vom *LG Berlin* verneint.[1054]

aa) Datenschutzrechtliche Verantwortlichkeit

Wenn ein Nutzer eines sozialen Netzwerks eine App oder sonstige Dienstleistung eines Drittanbieters verwenden möchte, wird er zunächst individuell darüber informiert, dass diese dann Zugriff auf seine Daten erhält. Facebook schreibt darüber hinaus in seinen Datenrichtlinien:

[1050] Facebook, Annual Report 2013, S. 48.

[1051] Facebook Inc., Form 10-k für die amerikanische SEC, abgegeben am 29.01.2015 für den Zeitraum bis 31.12.2014, S. 62; Facebook Annual Report 2014, S. 43.

[1052] Facebook, Annual Report 2015, S. 42.

[1053] Während man überlegen kann, ob dies eine den die App verwendenden Nutzern zuzurechnende Übermittlung darstellt, ist dies im Ergebnis abzulehnen, vgl. ausführlich oben unter D.I.3.b)bb)ii). Die datenschutzrechtliche Verantwortlichkeit muss somit – da es keine unverantworteten Datenverarbeitungen geben darf – entweder bei dem Anbieter des sozialen Netzwerks und/oder den App-Anbietern liegen.

[1054] LG Berlin, ZD 2015, 133 (135); vgl. auch *Boos*, VuR 2015, 92 (94 ff.).

> *„Wenn du Apps, Webseiten oder sonstige Dienste Dritter verwendest, die unsere Dienste nutzen bzw. auf diesen integriert sind, erhalten sie möglicherweise Informationen darüber, was du postest oder teilst. Wenn du beispielsweise ein Spiel mit deinen Facebook-Freunden spielst oder den Facebook-Button „Kommentieren" bzw. „Teilen" auf einer Webseite verwendest, kann der Spieleentwickler bzw. die entsprechende Webseite Informationen über deine Aktivitäten in dem Spiel erhalten, oder der Entwickler sieht einen Kommentar oder Link, den du von seiner Webseite auf Facebook teilst. Beim Herunterladen bzw. durch ihre Nutzung können solche Dienste Dritter darüber hinaus auf dein Öffentliches Profil zugreifen; dieses umfasst deine/n Benutzernamen oder Nutzer-ID, deine Altersgruppe und dein Land bzw. deine Sprache, deine Freundesliste sowie jedwede Informationen, die du mit ihnen teilst. Die von diesen Apps, Webseiten oder integrierten Diensten gesammelten Informationen unterliegen deren eigenen Nutzungsbedingungen und Richtlinien."*[1055]

Die Anbieter der Apps erhalten somit Zugriff auf zahlreiche Daten der Nutzer. Da diese Apps in ähnlicher Form auf Facebook eingebunden sind wie Fanpages, erscheint die Annahme plausibel, dass es auch bei ihrer Verwendung zu einer Erhebung von Bestands- und Nutzungsdaten durch Facebook kommt und die so gewonnenen Daten entsprechend von Facebook zur Bildung von Nutzungsprofilen verwendet werden. Sollte dies zutreffen – die Beantwortung dieser Frage muss der Forschung im Bereich der Informatik vorbehalten bleiben – so spricht Vieles dafür, den Anbietern dieser Apps die gleiche mittelbare datenschutzrechtliche Verantwortlichkeit für eine durch Facebook erfolgende Datenverarbeitung zuzusprechen wie Fanpage-Betreibern.

Soweit die Anbieter solcher Apps, anders als Fanpage-Betreiber und Verwender von Social PlugIns, einen direkten Zugriff auf von Facebook gespeicherte Profil-, Bestands- und Nutzungsdaten erhalten, sind sie für den Umgang mit den dadurch verfügbaren Daten in jedem Fall vollständig datenschutzrechtlich verantwortlich.[1056] Dies gilt erst Recht, wenn sie Kopien der Profildaten auf eigenen Servern speichern. Die Anbieter dieser Apps benötigen in diesen Fällen eine gesetzliche Erlaubnis für die Verarbeitung dieser Daten. Alternativ kann ihnen die Verarbeitung auch durch eine Einwilligung gestattet werden. Es muss daher im praktischen Einzelfall untersucht werden, ob ein Erlaubnistatbestand nach §§ 28, 29 BDSG bzw. Art. 6 Abs. 1 lit. b)-f) DS-GVO für die Verarbeitung einschlägig ist oder eine wirksame Einwilligung erklärt wurde.[1057] Hierfür sollen im Folgenden allgemeine Leitlinien aufgezeigt werden.

[1055] https://www.facebook.com/privacy/explanation (Stand 29. September 2016).

[1056] Vgl. allgemein für Entwickler von Apps auf Smart Devices: Art. 29 DatSchGruppe, Stellungnahme 02/2013, WP 202, S. 10.

[1057] Vgl. hierzu *Boos*, VuR 2015, 92 (95 ff.).

bb) Erlaubnistatbestände

Generalisiert betrachtet kommen als gesetzliche Erlaubnisnormen nur § 28 Abs. 1 Nr. 2 BDSG bzw. § 29 Abs. 1 Nr. 1 BDSG und zukünftig Art. 6 Abs. 1 lit. f) DS-GVO in Betracht, so dass es zur Beurteilung der Rechtmäßigkeit auf eine Interessenabwägung im Einzelfall ankommt. Entscheidend sind hierbei insbesondere der konkrete Umfang der Daten, auf welche zugegriffen wird, und ihre Erforderlichkeit für die vom Nutzer gewünschte Dienstleistung. § 28 Abs. 1 Nr. 1 BDSG wird dagegen ebenso wie Art. 6 Abs. 1 lit. b) DS-GVO regelmäßig ausscheiden, da jedenfalls die ganz überwiegende Menge der verarbeiteten Profildaten nicht für eine Vertragsbegründung erforderlich ist.[1058]

Soweit es sich um Angaben des öffentlichen Profils innerhalb Facebooks handelt, liegen allgemein zugängliche Daten im Sinne von § 28 Abs. 1 Nr. 3 BDSG bzw. § 29 Abs. 1 Nr. 2 BDSG vor, die auch im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO geringer zu gewichten sind. Das öffentliche Profil ist grundsätzlich jeder Person zugänglich, die bei Facebook registriert ist – ein Verbergen dieses Profils ist innerhalb des Netzwerks nicht möglich. Es kann darüber hinaus sogar dem gesamten Internet zugänglich sein, wenn in den Privatsphäre-Einstellungen eine Auffindbarkeit über Suchmaschinen auch außerhalb Facebooks gestattet wurde.[1059] Soweit die Daten über das gesamte Internet abrufbar sind, handelt es sich zweifelsohne um allgemein zugängliche Daten.[1060] Sehr verbreitet wird dies aber auch für netzwerköffentliche Daten bejaht, da das Registrierungserfordernis keine relevante Zugangshürde darstellt.[1061]

[1058] So auch LG Berlin, ZD 2015, 133 (135); Art. 29 DatSchGruppe, Stellungnahme 15/2011, WP 187, S. 22.

[1059] Facebook informiert hierzu: „Inhalte, die öffentlich sind, können von jedem gesehen werden. Dazu zählen auch Personen, die nicht deine Freunde sind, die Facebook nicht nutzen und die Inhalte über andere Medien wie Druckmedien, Rundfunk (z. B. Fernsehen) und andere Webseiten im Internet ansehen. […] Einige Informationen, die du uns zur Verfügung stellst, wenn du dein Profil erstellst, sind öffentlich, z. B. dein Alter, dein Geschlecht, deine Sprache und dein Land. Darüber hinaus verwenden wir teilweise Informationen deines Profils, des sogenannten „öffentlichen Profils", damit du leichter mit deinen Freunden und deiner Familie in Kontakt treten kannst. *Dein öffentliches Profil umfasst deinen Namen, dein Geschlecht, deinen Nutzernamen und die Nutzer-ID (Kontonummer), Profilbild, Titelbild und deine Netzwerke.* [Hervorhebung der Verfasserin] Diese Informationen sind ebenfalls öffentlich." https://www.facebook.com/help/958948540830352/ unter „Was sind öffentliche Informationen?".

[1060] *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 82; *Simitis*, in: Simitis, BDSG, § 28 Rn. 151; *Kramer*, in: Auernhammer, § 28 BDSG, Rn. 20; *Wolff*, in: Wolff/Brink, § 28 BDSG, Rn. 83; *Wedde*, in: DKWW, § 28 BDSG, Rn. 58.

[1061] *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 83; *Kramer*, in: Auernhammer, § 28 BDSG, Rn. 20; *Plath*, in: Plath, § 28 BDSG, Rn. 76; a.A. *Wolff*, in: Wolff/Brink, § 28 BDSG, Rn. 83; *Wedde*, in: DKWW, § 28 BDSG, Rn. 58; hierzu auch bereits oben unter D.I.3.a)cc).

Ein genauer Abgleich der laut Facebooks Datenrichtlinie an Drittanbieter übermittelten Daten mit den im öffentlichen Profil angezeigten Daten zeigt indes, dass erstere über letztere hinausgehen. So erklärt Facebook – wie oben mit Fn. 1055 zitiert –, dass auch die Altersgruppe, die Sprache, die Freundesliste sowie Inhalte, die mit Freunden geteilt wurden, an die Anbieter von Apps und vergleichbaren Dienstleistungen übermittelt werden. Diese Angaben zählen aber, wie aus dem Zitat in Fn. 1059 ersichtlich wird, nicht zu den Informationen, die im für alle sichtbaren öffentlichen Profil enthalten sind. Dies bestätigt auch eine stichprobenartige Überprüfung öffentlich sichtbarer Profile bei Facebook. Facebook verwendet hier vielmehr in sehr missverständlicher Weise einen identischen Begriff, konkret den des „öffentlichen Profils", für unterschiedliche Konzepte und Vorgänge.[1062]

Selbst wenn man die innerhalb des sozialen Netzwerks öffentlich zugänglichen Daten unter § 28 Abs. 1 Nr. 3 BDSG bzw. § 29 Abs. 1 Nr. 2 BDSG subsumiert, ist die stattfindende Datenübermittlung an Drittanbieter daher jedenfalls nicht vollständig von diesen Normen erfasst, da diese auch nicht-öffentliche Daten umfasst. Maßgeblich ist vielmehr eine Interessenabwägung gemäß § 28 Abs. 1 Nr. 2 BDSG bzw. § 29 Abs. 1 Nr. 1 BDSG. Auch diese Normen kommen indes nur dann als Erlaubnistatbestand in Frage, wenn entgegen aller Zweifel die vorherige Übermittlung der Daten durch Facebook an den App-Anbieter als rechtmäßig eingestuft wird. Andernfalls würde man die Möglichkeit einer rechtmäßigen Weiterverarbeitung rechtswidrig erlangter Daten schaffen, was eine unzumutbare Beeinträchtigung von Betroffenenrechten darstellen würde. Dies wäre entsprechend auch bei der Interessenabwägung gemäß Art. 6 Abs. 1 lit. f) DS-GVO zu berücksichtigen.

Soweit auch nach der Interessenabwägung gemäß §§ 28 Abs. 1 Nr. 2, 29 Abs. 1 Nr. 1 BDSG bzw. Art. 6 Abs. 1 lit. f) DS-GVO keine Erlaubnis vorliegt, kann die Datenverarbeitung nur durch eine Einwilligung legitimiert sein. Eine solche muss hinreichend informiert abgegeben werden. Zudem muss die Einwilligung eingeholt worden sein, bevor Daten bereits verarbeitet wurden, und dem Nutzer muss eine klare und eindeutige Möglichkeit gegeben werden, die Installation oder Nutzung der App abzubrechen, wenn er diese Datenverarbeitung nicht wünscht.[1063]

Bei der Einholung der Einwilligung ist zu differenzieren zwischen der Verarbeitung der Daten des die App verwendenden Nutzers und der Daten seiner Kontakte. Bereits hinsichtlich des die

[1062] Vgl. bereits ausführlich *Boos*, VuR 2015, 92 (94 f.).

[1063] Vgl. ausführlich Art. 29 DatSchGruppe, Stellungnahme 02/2013, WP 202, S. 14 ff.; Art. 29 DatSchGruppe, Stellungnahme WP 187, S. 22.

App verwendenden Nutzers bestehen gewichtige Zweifel, ob die Einwilligung in die Datenweitergabe durch Facebook und die anschließende Verarbeitung durch den App-Anbieter wirksam ist.[1064] Die Aufklärung erfolgt häufig in einem sehr langen, wenig verständlichen Text, was ihre Effektivität bereits grundsätzlich in Frage stellt.[1065] Zudem verleitet die Gestaltung des Informationsfeldes den Nutzer dazu, die Aufklärung über die Datenverarbeitung nicht sehr ernst zu nehmen, sondern stattdessen direkt die Anwendung zu nutzen.[1066] Dies gilt umso mehr, als es sich bei diesen Apps und vergleichbaren Dienstleistungen häufig um kleine Spiele handelt, bei denen der Spieltrieb der Nutzer gezielt angesprochen wird. Ihnen ist daher nicht notwendig bewusst, dass es sich bei dieser von ihnen als verhältnismäßig unwichtig und nur zum Spaß vorgenommenen Handlung um eine Einwilligung in eine umfassende Datenverarbeitung handeln kann.[1067] Das *LG Berlin* hat entsprechend die Wirksamkeit der Einwilligung verneint.[1068]

Jedenfalls nicht von einer Einwilligung gedeckt ist der Zugriff auf die Profildaten von Kontakten der die App verwendenden Nutzer. Dass ein solcher Zugriff stattfindet, ist – wie bereits oben in der Diskussion zur Verantwortlichkeit der Nutzer dargelegt – spätestens seit 2011 durch das Audit des irischen Datenschutzbeauftragen bekannt.[1069] Auch Facebook selbst bietet den Betroffenen ausdrücklich an, dies zu unterbinden, indem sie sich einer Nutzung der Angebote von Drittanbietern vollständig verweigern.[1070] Es handelt sich also um ein „Alles-oder-Nichts-Prinzip“: Die aktive eigene Verwendung der Dienstleistungen Dritter ist nur möglich, wenn man auch der passiven Datenübermittlung zustimmt, die automatisch erfolgt, wenn Kontakte derartige Dienstleistungen Dritter verwenden. Die Einwilligung in diese Konditionen bedeutet im Endeffekt einen vollständigen Kontrollverlust des Betroffenen über

---

[1064] *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 78; allgemein zu Problemen der Einwilligung auch noch ausführlich unten unter D.III.2.b)aa)..

[1065] *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 78.

[1066] LG Berlin, ZD 2015, 133 (134); *Boos*, VuR 2015, 92 (96).

[1067] LG Berlin, ZD 2015, 133 (134); *Boos*, VuR 2015, 92 (96); *Heckmann*, NJW 2012, 2631 (2633 f.).

[1068] LG Berlin, ZD 2015, 133 (134 f.): ausführlich zu Fragen der Wirksamkeit der Einwilligung noch unten unter D.III.2.b). Freilich kann man sich die Frage stellen, wie sich dieses Ergebnis zu dem insbesondere im Verbraucherschutzrecht verbreiteten Bild des „mündigen Verbrauchers“ bzw. hier des Nutzers verhält. Letztendlich wird man anerkennen müssen, dass es sich bei der durch dieses Ideal postulierten vernünftigen Abwägung von Optionen häufig um eine Fiktion handeln wird, gerade wenn – wie hier – der Spieltrieb planvoll angesprochen und die datenschutzrechtlichen Risiken sehr schwer einzuschätzen sind. Hierzu auf konzeptioneller Ebene noch vertieft unten unter E.II.

[1069] *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 90 f.

[1070] In den Einstellungen zu „von anderen Personen verwendeten Apps“ formuliert Facebook hierzu: „Falls du nicht möchtest, dass Apps und Webseiten Zugriff auf andere Kategorien von Informationen (z. B. deine Freundesliste, dein Geschlecht oder andere Informationen, die du öffentlich zugänglich gemacht hast) haben, dann deaktiviere alle Plattform-Apps. Beachte aber, dass du dann selber keine Apps und Spiele mehr nutzen kannst.“ https://www.facebook.com/settings?tab=applications.

die derart weitergegebenen Daten, da für den Betroffenen in keiner Weise ersichtlich und absehbar ist, welche Dienstleistungen ihre Kontakte verwenden werden und an welche Stellen ihre Daten daher übermittelt werden.[1071] Entsprechend sieht sich diese Regelung Facebooks auch seit Jahren erheblicher datenschutzrechtlicher Kritik ausgesetzt[1072], freilich ohne dass dies bisher eine entscheidende Änderung bewirkt hätte.

Eine wirksame Einwilligung der Betroffenen scheitert somit regelmäßig daran, dass sie nicht hinreichend informiert erfolgt.[1073] Die beschriebene Datenverarbeitung erfolgt in einer sehr abstrakten Dreieckskonstellation. Facebook weist seine Nutzer in keiner Weise angemessen darauf hin, dass sie durch die eigene Nutzung einer App auch allen Apps und Dienstleistungen ihrer Kontakte Zugriff auf ihre Profildaten gewähren. Die hierzu verfügbaren Hinweise sind vielmehr versteckt und abstrakt gehalten. Es handelt sich zudem um überraschende, die Nutzer unangemessen benachteiligende Klauseln.[1074] Insbesondere ist, wie ebenfalls bereits angedeutet wurde, das Auffinden der Opt-Out-Einstellung alles andere als intuitiv.[1075] Sie kann nämlich nicht über die Privatsphäre-Einstellungen[1076] aufgerufen werden, sondern nur über die allgemeinen Kontoeinstellungen und dort über das Untermenü der App-Einstellungen[1077].

Selbst wenn Betroffene durch eine aktive eigene Nutzung von Apps und Dienstleistungen Dritter vermeintlich in die Übermittlung ihrer Daten durch Apps verwendende Kontakte einwilligen, ist diese Einwilligung daher nicht wirksam. Sofern nicht einmal dieser Anknüpfungspunkt vorliegt, sondern sich eine Einwilligung aus einem unterlassenen Opt-Out ergeben soll, ist dies erst Recht abzulehnen. Es wäre nachgerade absurd, eine freiwillige informierte Einwilligung in das Unterlassen des Opt-Out zu lesen, wenn nicht erwartet werden kann, dass den Betroffenen überhaupt bewusst ist, dass es zu dieser Form der Datenübermittlung kommen kann.

1071 LG Berlin, ZD 2015, 133 (134).

1072 *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 35; *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 90 f.; vgl. auch *Maisch*, Informationelle Selbstbestimmung, S. 229 ff.

1073 So auch *Maisch*, Informationelle Selbstbestimmung, S. 236; *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 43; LG Berlin, ZD 2015, 133 (134 f.); Boos, VuR 2015, 92 (96 f.).

1074 Vgl. LG Berlin, ZD 2015, 133 (135 f.).

1075 Kritisch hierzu auch schon *Irish Data Protection Commissioner*, Report of Re-Audit, 21.09.2012, S. 30 f.; *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 90 f.

1076 https://www.facebook.com/settings?tab=privacy.

1077 https://www.facebook.com/settings?tab=applications; vgl. auch *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 38.

cc) Zwischenergebnis

Von Dritten angebotene Dienstleistungen und Apps erweisen sich damit als datenschutzrechtlich relevante Elemente von sozialen Netzwerken, die bisher in der rechtswissenschaftlichen Forschung nur wenig bis kaum berücksichtigt wurden. Teile der durch sie vorgenommenen Datenverarbeitungen, insbesondere die Verarbeitung von Profildaten Dritter, sehen sich erheblichen Zweifeln an ihrer Rechtmäßigkeit ausgesetzt.

Das Datenschutzrecht kann den von ihnen gestellten Herausforderungen allerdings gerecht werden, da derartige Anbieter als unmittelbar datenschutzrechtlich Verantwortliche anzusehen sind, soweit sie selbst personenbezogene Daten verarbeiten. Ob ihnen darüber hinaus eine den Betreibern von Fanpages und Verwendern von Social PlugIns vergleichbare mittelbare Verantwortlichkeit für durch Facebook erfolgende Datenverarbeitung zukommt, ist insbesondere abhängig von dem Umfang und der Art der mit Facebook ausgetauschten Daten. Für eine abschließende Klärung dieser Frage ist daher zunächst weitere Forschung im Bereich der Informatik abzuwarten.

f) Zwischenfazit: Der Verantwortlichkeitsbegriff im Zusammenhang mit sozialen Netzwerken

Ausgangspunkt der Untersuchung war die Feststellung, dass das geltende Datenschutzrecht im Grundsatz von einem bipolaren Verhältnis eines Datenverarbeiters und eines hiervon Betroffenen ausgeht. Trotz eines sehr umfangreichen Gesetzgebungsprozesses sind in dieser Hinsicht keine konzeptionellen Neuerungen im Rahmen der DS-GVO festzustellen. In der vorstehenden Analyse konnte aber gezeigt werden, dass das Datenschutzrecht dennoch flexibel genug ist, um auch mit den mehrseitigen Rechtbeziehungen verschiedener Akteure und Datenverarbeiter in sozialen Netzwerken sinnvoll umzugehen.

Die Verantwortlichkeit einer datenverarbeitenden Stelle bestimmt sich nach ihrer Kontrolle über die Datenverarbeitung, also insbesondere nach ihrem Einfluss auf die Zwecke und Mittel, zu und mit denen diese erfolgt.

Anbieter sozialer Netzwerke erweisen sich hiernach als umfassend Verantwortliche für die innerhalb des Netzwerks erfolgende Datenverarbeitung. Während sie zwar nur eingeschränkte Kontrolle über die Auswahl und die Zwecksetzung der konkret übermittelten Daten haben – insbesondere im Fall von nutzergenerierten Inhaltsdaten über Dritte – dienen letztlich alle übermittelten Daten den Geschäftszwecken des Anbieters und seiner damit

zusammenhängenden Datenverarbeitung. Aufgrund des maßgeblichen funktionell-wirtschaftlichen Verantwortlichkeitsbegriffs sind Anbieter sozialer Netzwerke daher als umfassend datenschutzrechtlich verantwortlich anzusehen und Adressaten entsprechender ordnungsrechtlicher Pflichten.

Nutzer sozialer Netzwerke sind datenschutzrechtlich verantwortlich, wenn und soweit sie personenbezogene Daten über Dritte übermitteln. Sie sind nicht durch die Regelung des § 1 Abs. 2 Nr. 3 BDSG bzw. Art. 2 Abs. 2 lit. c) DS-GVO privilegiert, da die Verarbeitung von Daten in sozialen Netzwerken grundsätzlich nicht als persönliche oder familiäre Tätigkeit einzuordnen ist. Unabhängig von der Zahl der Adressaten bestehen Risiken der Verbreitung und langfristigen Speicherung der Daten, welche eine unverhältnismäßige Gefährdung der informationellen Selbstbestimmung der Betroffenen begründen. Die Gefährdungslage ist daher nicht mit der Risikoabwägung vereinbar, welche der grundsätzlichen Privilegierung zugrunde liegt. Nutzer sozialer Netzwerke sind insoweit ebenfalls Adressaten der datenschutzrechtlichen Pflichten, soweit sie diesen tatsächlich nachkommen können.

Besonders problematisch ist die datenschutzrechtliche Verantwortlichkeit der Anbieter von Fanpages für die von Facebook vorgenommene Verarbeitung der Bestands- und Nutzungsdaten, die bei dem Besuch einer Fanpage anfallen. Anders als teilweise in der Literatur angenommen, kommt den Fanpage-Betreibern keine unmittelbare Verantwortlichkeit hierfür zu. Sie sind auch keine Auftraggeber einer Auftragsdatenverarbeitung. Sie initiieren zwar die Erhebung der Daten, indem sie für Nutzer einen Anlass setzen, sich auf der Seite aufzuhalten; sie verfügen aber über keinen relevanten Einfluss auf die Zwecke und Mittel der daraus resultierenden Datenverarbeitung. Das Datenschutzrecht stößt hier an seine regulatorischen Grenzen, indem ein klarer Fall von Verantwortlichkeitsdiffusion durch Arbeitsteilung vorliegt. Ein effektiver Schutz von Betroffenenrechten und eine umfassende ordnungsrechtliche Regulierung ist aber durch einen Rückgriff auf die Grundsätze des allgemeinen Polizei- und Ordnungsrechts gewährleistet. Da das Datenschutzrecht nicht als abschließende Regelung der Verantwortlichkeit zu betrachten ist, besteht eine mittelbare Verantwortlichkeit als Zweckveranlasser, soweit es zu rechtswidrigen Datenverarbeitungsschritten durch Facebook kommt und die Fanpage-Betreiber hiervon wissentlich profitieren. Dies ist insbesondere im Zusammenhang mit der zur Verfügung gestellten Statistik Facebook Insights der Fall, welche u.a. unter Verstoß gegen das Trennungsgebot aus § 15 Abs. 3 TMG erstellt wird. Sie können damit jedenfalls Adressaten von ordnungsrechtlichen Verfügungen gemäß § 38 Abs. 5 BDSG sein, insbesondere soweit diese auf Unterlassung des datenschutzwidrigen Verhaltens gerichtet

sind. Eine vergleichbare Situation ergibt sich mit Anwendbarkeit der DS-GVO, nach welcher die Fanpage-Betreiber ebenfalls als mittelbar Verantwortliche Adressaten von Verfügungen der Aufsichtsbehörde sein können.

Als Sonderfall der Verwendung von Fanpages stellen sich Fanpages der öffentlichen Hand dar. Über die zur Verantwortlichkeit von privaten Fanpages hinaus getroffenen Feststellungen ist hier der Grundsatz der Bindung der Verwaltung an Recht und Gesetz gemäß Art. 20 Abs. 3 GG zu beachten. Die Verwaltung darf sich dieser Bindung nicht dadurch entziehen, dass sie von rechtswidrigem Verhalten eines privaten Akteurs profitiert. Konsequenterweise ist die Verwendung von Facebook-Fanpages durch die öffentliche Hand daher unter den gegenwärtigen Datenverarbeitungsbedingungen durch Facebook als unzulässig einzustufen.

Auch den Verwendern von Social PlugIns kommt mangels eines hinreichenden Einflusses auf die Zwecke und Mittel der Datenverarbeitung keine unmittelbare, vollständige datenschutzrechtliche Verantwortlichkeit für die durch Facebook erfolgende Verarbeitung der durch das Social PlugIn übermittelten Daten zu. Anders als die Fanpage-Betreiber haben die Verwender von Social PlugIns aber die Kontrolle darüber, ob es überhaupt zu einer automatischen Übermittlung der Daten kommt. Die Übermittlung der Daten über das Social PlugIn ist abhängig von seiner technischen Implementierung auf der externen Webseite, welche ausschließlich im Machtbereich des Webseitenbetreibers liegt. Soweit sie eine automatische Übermittlung von Nutzerdaten an Facebook beim Aufruf ihrer Webseite zulassen, sind sie daher mittelbar für die erfolgende Datenverarbeitung durch Facebook verantwortlich. Ihnen kommen entsprechend öffentlich-rechtliche und gegebenenfalls auch zivilrechtliche Unterlassungspflichten zu.

Die letzte untersuchte Gruppe von Akteuren sind die Anbieter von externen Inhalten, etwa Spielen oder Apps in sozialen Netzwerken. Eine präzise rechtliche Einordnung sieht sich vor allem dem Problem ausgesetzt, dass nicht abschließend geklärt ist, in welcher Form und in welchem Umfang personenbezogene Daten durch diese Anbieter verarbeitet werden. Sie sind jedenfalls unproblematisch als datenschutzrechtlich Verantwortliche einzustufen, sofern sie selbst nach eigener Entscheidungskompetenz personenebezogene Daten verarbeiten. Für darüber hinausgehende Feststellungen zu einer mittelbaren Verantwortlichkeit ist aber zunächst noch weitere Forschung im Fachbereich der Informatik erforderlich.

Es zeigt sich damit, dass trotz der komplexen mehrseitigen und arbeitsteiligen Akteursgeflechte in sozialen Netzwerken eine klare Zuweisung von Verantwortlichkeit und damit auch die Durchsetzung von datenschutzrechtlichen Vorschriften möglich ist.

II. Spannungsverhältnis zwischen Persönlichkeitsrechtsschutz und Rechtsverfolgung: Recht auf anonyme Nutzung?

Auch im Internet ist es erforderlich, Rechtsverletzungen verfolgen und ahnden zu können und einen Verantwortlichen für die Einhaltung von Pflichten benennen zu können. Dieser Notwendigkeit wird in der Regel u.a. durch ein Impressum Rechnung getragen, aus dem der verantwortliche Diensteanbieter offenbar wird.[1078] Die neueren technischen Entwicklungen gerade in sozialen Netzwerken machen es aber möglich, dass ein Diensteanbieter zugleich Nutzer eines Dienstes sein kann, es also die neue Kategorie eines gleichsam „diensteanbietenden Nutzers“ gibt.[1079] In dieser Konstellation kommt es zu einem Konflikt zwischen einer möglichen Impressumspflicht – die notwendig die Identität gegenüber weiteren Nutzern offenlegt – und dem in § 13 Abs. 6 TMG geregelten Recht auf anonyme bzw. zumindest pseudonyme Nutzung von Telemediendiensten. Die Reichweite der Impressumspflicht in sozialen Netzwerken ist daher umstritten.[1080] Entsprechend soll nun untersucht werden, inwieweit diese sich gegenseitig ausschließenden Regelungen miteinander in Einklang gebracht werden können.

1. Impressumspflicht in sozialen Netzwerken

Soweit Nutzer sozialer Netzwerke ihre Profilseite geschäftsmäßig als Diensteanbieter im Sinne des § 2 Nr. 1 TMG betreiben, unterliegen sie einer Impressumspflicht gemäß § 5 Abs. 1 TMG.[1081] Sie sind demnach unter anderem verpflichtet, ihren (realen) Namen und ihre Adresse bekannt zu machen. Auf welche Art dies (design-)technisch erfolgen muss, um den Erfordernissen der unmittelbaren Erreichbarkeit zu genügen, insbesondere ob eine

---

[1078] *Micklitz/Schirmbacher*, in: Spindler/Schuster, § 5 TMG, Rn. 2 m.w.N.; vgl. auch *Brönneke*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, § 6 TDG, Rn. 1 ff.

[1079] Hierzu bereits ausführlich oben unter D.I.3.b)cc). Zum hieraus resultierenden Konflikt mit dem Recht auf anonyme Nutzung gemäß § 13 Abs. 6 TMG unten unter D.II.2.b)dd).

[1080] Vgl. *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1, Rn. 2 ff.

[1081] OLG Düsseldorf, K&R 2013, 594 (595), Rn. 28; OLG Düsseldorf, MMR 2008, 682 (683); OLG Frankfurt, CR 2007, 454 (454); *Micklitz/Schirmbacher*, in: Spindler/Schuster, § 5 TMG Rn. 19; *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG, Rn. 11; *Pießkalla*, ZUM 2014, S. 368 (369); *Richter*, MMR 2014, S. 517 (517); *Lorenz*, VuR 2014, S. 83 (83), der allerdings nachfolgend ebendiese Eigenschaft als Diensteanbieter im Falle von Nutzern sozialer Netzwerke verneint; *Rockstroh*¸ MMR 2013, 627 (629 f.); *Stadler*, ZD 2011, 57 (58); *Schröder/Hawxwell*, Verletzung datenschutzrechtlicher Bestimmungen, in: Wissenschaftlicher Dienst des BT, S. 15; ausführlich zur Eigenschaft als Diensteanbieter oben unter D.I.3.b)cc).

Veröffentlichung unter den allgemeinen Profilinformationen genügt oder ob es hierfür eine eigene Impressumsrubrik geben muss[1082], soll hier nicht vertiefend erörtert werden.

§ 5 TMG ist die Neuregelung der Vorgängervorschrift in § 6 TDG, welche die Vorgaben des Art. 5 Abs. 1 ECRL umsetzte.[1083] Er stellt daher keine allgemeine datenschutzrechtliche Norm dar und wird entsprechend nicht durch die DS-GVO verdrängt werden. Selbst wenn man der Norm einen datenschutzrechtlichen Gehalt beimessen wollte, würde sich durch die enge Verbindung mit dem Recht des elektronischen Geschäftsverkehrs *e contrario* aus Art. 95 DS-GVO ergeben, dass eine Anwendbarkeit der DS-GVO in diesem Bereich nicht vom Verordnungsgeber intendiert war. Die DS-GVO hat daher keine Auswirkungen auf die Geltung des § 5 TMG und die folgenden Ausführungen.

Natürliche Personen, die ihr Profil allein zur persönlichen Kontaktpflege und Selbstdarstellung nutzen, sind mangels eines wirtschaftlichen Bezugs ihrer Tätigkeit bereits nicht als Diensteanbieter im Sinne von § 2 Nr. 1 TMG einzustufen.[1084] Selbst wenn man dies bestreiten wollte, unterliegen sie mangels Geschäftsmäßigkeit des Angebots jedenfalls nicht der Impressumspflicht nach § 5 Abs. 1 TMG. Der Begriff der Geschäftsmäßigkeit ist im TMG nicht legaldefiniert. Vereinzelt wurde in der Vergangenheit vertreten, ihn so eng zu verstehen, dass er nur berufliche oder gewerbliche Zwecke umfasst.[1085] Ganz überwiegend wird er heute dagegen so interpretiert, dass das Angebot eines Telemediums geschäftsmäßig ist, wenn es „nachhaltig", also auf einen längeren Zeitraum ausgerichtet und nicht auf Einzelfälle beschränkt ist.[1086] Auf eine Gewinnerzielungsabsicht soll es nicht ankommen. Diese Auslegung entspricht dem Wortlaut der Vorschrift, die nur auf „in der Regel gegen Entgelt angebotene Telemedien" abstellt, diese mithin nicht immer fordert.[1087]

Nach dem ausdrücklichen Willen des Gesetzgebers in der Gesetzesbegründung sollten indes „Telemedien, die ohne den Hintergrund einer wirtschaftlichen Tätigkeit bereitgehalten werden (z.B. Homepages, die rein privaten Zwecken dienen und die nicht Dienste breitstellen, die sonst nur gegen Entgelt verfügbar sind, oder entsprechende Informationsangebote von Idealvereinen), künftig nicht mehr den Informationspflichten des Telemediengesetzes"

[1082] Instruktiv hierzu: *Pießkalla*, ZUM 2014, S. 368 (S. 371); *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1, Rn. 3.
[1083] BT-Drs. 16/3078, S. 14; *Brönneke*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, § 6 TDG, Rn. 17.
[1084] Dazu oben unter D.I.3.b)cc)ii).
[1085] Vgl. die Nachweise bei *Micklitz/Schirmbacher*, in: Spindler/Schuster, § 5 TMG Rn. 8, dort Fn. 23.
[1086] *Micklitz/Schirmbacher*, in: Spindler/Schuster, § 5 TMG Rn. 8; *Rockstroh*¸ MMR 2013, 627 (630).
[1087] *Micklitz/Schirmbacher*, in: Spindler/Schuster, § 5 TMG Rn. 8; vgl. auch *Ott*, MMR 2007, 354 (355).

unterliegen.[1088] Ausschließlich auf die Nachhaltigkeit des Angebots abzustellen, erweist sich insoweit als ein ungeeignetes Kriterium, um diesen gesetzgeberischen Willen umzusetzen. Während es in den 1990er und zu Beginn der 2000er Jahre noch unüblich gewesen sein mag, dass private Akteure persönliche und strikt nicht-wirtschaftliche Profile und Webseiten im Internet betreiben – bzw. überhaupt die Gelegenheit für eine derartige öffentlichkeitswirksame Selbstdarstellung haben – ist dies heute nicht zuletzt durch soziale Netzwerke sogar eher die Regel denn die Ausnahme.[1089] Derartige private Profile sind regelmäßig auf einen längeren Zeitraum ausgerichtet, da sie der fortdauernden persönlichen Selbstinszenierung im Netz und der Kontaktmöglichkeit dienen. Im Ergebnis würde sich daher fast jedes Angebot im Internet als geschäftsmäßig erweisen. Dies würde das Kriterium entsprechend gegenstandslos werden lassen und zu einer allgemeinen Impressumspflicht unabhängig von einem wirtschaftlichen Bezug führen.

Das war jedoch ausweislich der Gesetzesbegründung[1090] nicht Absicht des nationalen Gesetzgebers und ausweislich der Erwägungen in der zugrundeliegenden E-Commerce-Richtlinie auch nicht Ziel der Reform. Vielmehr stellt auch Erwägungsgrund 18 ECRL ausdrücklich darauf ab, dass Dienste nur erfasst sind, „soweit es sich überhaupt um eine wirtschaftliche Tätigkeit handelt“. Der Verzicht auf ein direktes Entgeltlichkeitserfordernis liegt nicht zuletzt darin begründet, dass es auch Dienste wie etwa Internetsuchmaschinen oder Informationsdienste gibt, deren Nutzung nicht durch den Nutzer vergütet wird, sondern sich aus anderen Quellen wie etwa der Werbung finanziert.[1091] Insoweit sollten Umgehungen vermieden werden.

Um die „Geschäftsmäßigkeit“ eines Angebots zu beurteilen genügt es daher nicht, auf die Dauerhaftigkeit der Internetpräsenz abzustellen, sondern es muss auch ein zumindest irgendwie gearteter wirtschaftlicher Bezug insbesondere der beworbenen Leistung vorhanden sein.[1092] Dieser muss sich nicht unbedingt auf berufliche oder gewerbliche Zwecke beschränken, umfasst aber keine rein privaten und persönlichen Tätigkeiten.

[1088] BT-Drs. 16/3078, S. 14; *Hoeren*, NJW 2007, S. 801 (803); teilweise a.A. wohl *Ott*, MMR 2007, 354 (355), dem zufolge bereits eine übliche Refinanzierung einer privaten Homepage durch das Schalten von Werbeanzeigen Dritter zu einer Entgeltlichkeit führen soll.

[1089] Vgl. zur gesellschaftlichen Bedeutung sozialer Netzwerke bereits oben unter B.I.2.

[1090] BT-Drs. 16/3078, S. 14.

[1091] Vgl. auch *Ott*, MMR 2007, 354 (355).

[1092] *Micklitz/Schirmbacher*, in: Spindler/Schuster, § 5 TMG Rn. 11; *Rockstroh*¸ MMR 2013, 627 (629); *Ott*, MMR 2007, 354 (355).

Ein systematisches Argument für diese einschränkende Auslegung des Begriffs der Geschäftsmäßigkeit in § 5 Abs. 1 TMG ergibt sich auch aus § 55 Abs. 1 RStV, welcher Telemedien, die nicht ausdrücklich persönlichen oder familiären Zwecken dienen, einer eingeschränkten Impressumspflicht unterwirft. Wären solche Zwecke aufgrund einer Dauerhaftigkeit des Angebots bereits von § 5 Abs. 1 TMG erfasst, wäre diese Norm materiell gegenstandslos und nur für Zuständigkeitsfragen hinsichtlich der Überwachung der Einhaltung relevant.[1093] Die Begründung zum 9. Rundfunkänderungsstaatsvertrag (RÄStV) weist indes ausdrücklich darauf hin, dass diese Ausnahmeregelung dem Schutz der Privatsphäre dienen soll, um zu verhindern, dass Personen durch eine allgemeine Impressumspflicht von privater Kommunikation abgeschreckt werden.[1094] Nicht der Kennzeichnungspflicht unterliegt daher „private Kommunikation, auch wenn sie über reine Telekommunikation hinausgeht", wie etwa bei einer „Einstellung von Meinungsäußerungen in Foren", aber auch Kommunikation im Rahmen eines „gelegentlichen privaten wirtschaftlichen Geschäftsverkehr[s], etwa bei der Veräußerung von Waren, unmittelbar durch den privaten Anbieter oder aber über dritte Plattformen".[1095] Die schutzwürdigen Belange anderer Nutzer würden in diesem Fall entweder durch eine private Bekanntschaft der Nutzer oder aber über den Plattformanbieter abgesichert.[1096]

Die Begründung stellt zwar nicht ausdrücklich auf private Profile in sozialen Netzwerken ab. Dies scheint aber nicht einer bewussten Entscheidung des Gesetzgebers geschuldet zu sein, sondern vielmehr der Tatsache, dass im Jahr 2006, als diese Änderung vorgenommen wurde, soziale Netzwerke schlicht weniger verbreitet waren und nicht als eigenständige Problematik wahrgenommen wurden.[1097] Gerade der Verweis auf die Interessenwahrung anderer Nutzer über die Einbindung des Plattformanbieters lässt plausibel erscheinen, dass auch rein private Profile in sozialen Netzwerken grundsätzlich nicht der Impressumspflicht unterliegende Telemedien darstellen. Denn wie oben unter I.3.a)aa)D.I.3.a) bereits gezeigt wurde, besteht eine weitgehende Anbieterverantwortlichkeit für nutzergenerierte Inhalte sowohl in Bezug auf das

[1093] So *Hoeren*, NJW 2007, S. 801 (803).
[1094] LT-BW-Drs. 14/558, S. 39.
[1095] LT-BW-Drs. 14/558, S. 38 f.; siehe auch *Micklitz/Schirmbacher*, in: Spindler/Schuster, § 55 RStV, Rn. 11 ff.
[1096] LT-BW-Drs. 14/558, S. 39; kritisch *Richter*, MMR 2014, 517 (519 f.) für Plattformen, in denen aufgrund nicht verifizierter Registrierungsverfahren via Email keine sichere Zuordnung möglich sei. *Richter* übergeht hierbei allerdings die Möglichkeit, eine Zuordnung der Identität über ein Auskunftsersuchen bei dem Access-Provider hinsichtlich der IP-Adresse vorzunehmen. Zudem wäre es ein besserer Interessenausgleich, im Innenverhältnis zum Plattformbetreiber eine (überprüfbare) Registrierung unter dem Klarnamen zu verlangen, im Verhältnis gegenüber anderen Nutzern aber eine pseudonyme Nutzung ohne öffentliche Angabe der in § 55 RStV geforderten Daten zu ermöglichen, hierzu sogleich ausführlicher unter D.II.2.c).
[1097] Vgl. zur Verbreitung von sozialen Netzwerken oben unter B.I.2.

Datenschutzrecht als auch allgemein nach den §§ 7 ff. TMG. Der Telos der Impressumspflicht, nämlich in einem möglicherweise wirtschaftlich relevanten Zusammenhang einen rechtlich Verantwortlichen benennen bzw. ermitteln zu können, ist damit gewahrt.

Rein private Profile in sozialen Netzwerken sind teleologisch betrachtet Fortentwicklungen privater Webseiten, die nach der Gesetzesbegründung zu § 5 Abs. 1 TMG mangels einer wirtschaftlichen Tätigkeit gerade nicht Regelungsgegenstand der Impressumspflicht sein sollten.[1098] Sie sind zudem in Plattformen eingebunden, deren Anbieter ihrerseits einer geschäftsmäßigen Impressumspflicht unterliegen. Entsprechend weisen sie auch den in der Begründung des 9. RÄStV geforderten Ausnahmecharakter auf, die darauf abzielt, über diesen Plattformanbieter die Interessen der Betroffenen regeln zu können.[1099] In zeitgemäßer Auslegung des Willens des Gesetzgebers sind sie weder von der Impressumspflicht gemäß § 5 Abs. 1 TMG noch gemäß § 55 Abs. 1 RStV erfasst.[1100]

Dies ist auch mit der in dieser Arbeit vertretenen Auslegung des Begriffs der persönlichen und familiären Tätigkeit im Rahmen des Haushaltsprivilegs gemäß § 1 Abs. 2 Nr. 3 BDSG bzw. Art. 2 Abs. 2 lit. c) DS-GVO vereinbar.

Wie oben unter D.I.3.b)aa) dargelegt wurde, fällt die Verarbeitung, Nutzung oder Erhebung personenbezogener Daten auch in rein privat genutzten Profilen in sozialen Netzwerken regelmäßig nicht unter das Haushaltsprivileg gemäß § 1 Abs. 2 Nr. 3 BDSG bzw. Art. 2 Abs. 2 lit. c) DS-GVO, da sie nicht im Rahmen rein persönlicher oder familiärer Tätigkeiten im Sinne dieser Vorschrift erfolgt. Es mag sich nicht unmittelbar erschließen, warum nun im Rahmen von § 55 Abs. 1 RStV in derselben Konstellation das Vorliegen von ausschließlich familiären oder persönlichen Zwecken bejaht werden soll. Gerade im Verhältnis zur nationalen Norm des § 1 Abs. 2 Nr. 3 BDSG könnte dies wie ein Widerspruch im Rahmen der Einheit der Rechtsordnung wirken. Eine solche gespaltene Auslegung des *prima facie* identischen Begriffes ist indes aufgrund des unterschiedlichen teleologischen Ansatzpunktes der beiden Normen geboten.

1098 BT-Drs. 16/3078, S. 14.

1099 LT-BW-Drs. 14/558, S. 39.

1100 So auch *Micklitz/Schirmbacher*, in: Spindler/Schuster, § 5 TMG Rn. 20; *Rockstroh*¸ MMR 2013, 627 (630); a.A. *Ott*, MMR 2007, 354 (356); *Richter*, MMR 2014, 517 (518 f.), mit dem Argument, dass Profile in sozialen Netzwerken regelmäßig nicht ausschließlich persönlichen oder privaten Zwecken i.S.v. § 55 Abs. 1 RStV dienten.

Telos des BDSG ist es, jede Form der Datenverwendung, die nicht durch eine Einwilligung oder gesetzliche Erlaubnis gedeckt ist, zu untersagen, um eine Verletzung der informationellen Selbstbestimmung zu verhindern; nicht die Verweigerung einer Einwilligung, sondern der Zugriff auf fremde Daten ist rechtfertigungsbedürftig.[1101] Datenverarbeitungen im Rahmen von rein persönlichen und familiären Tätigkeiten sind nur deshalb ausgenommen, weil der Eingriff mangels einer großen Verbreitung der Daten regelmäßig geringfügig ist – wobei es auf die Intensität des Eingriffs im Einzelfall aber nicht ankommt – und die privaten Interessen und Freiheiten des Datenverarbeiters als grundsätzlich gleichwertig zu der informationellen Selbstbestimmung des Betroffenen einzustufen sind.[1102] Die Regelungen des RStV zielen dagegen darauf ab, rechtlich Verantwortliche im Falle einer Rechtsverletzung im Rahmen des Telemediengebrauchs bestimmen zu können sowie einen offenen Meinungsbildungsprozess und Verbraucherschutz zu ermöglichen.[1103] Sie dienen einer Abgrenzung von geschäftsmäßigen, wenngleich nicht notwendig gegen Entgelt angebotenen Aktivitäten und Aktivitäten, die zu rein privaten, persönlichen oder familiären Zwecken erfolgen.[1104] Anders als bei der Abgrenzung nach dem BDSG kommt es bei der Abgrenzung nicht darauf an, ob nur ein sehr geringer Verbreitungsgrad ohne Öffentlichkeitswirksamkeit zu erwarten ist. Dies ergibt sich insbesondere aus der Gesetzesbegründung, die die Ausnahme ausdrücklich auch auf private Tätigkeit in Meinungsforen und Verkaufsplattformen bezieht, die sogar einen sehr hohen Verbreitungsgrad erzielen können.[1105]

Formen der Datenverwendung, auf die sich das BDSG mit der Ausnahme in § 1 Abs. 2 Nr. 3 BDSG bezieht, würden mangels Verbreitung und Zugänglichkeit in aller Regel noch keine Telemedienangebote darstellen, die vom RStV überhaupt erfasst wären. Die Legaldefinition des Rundfunks in § 2 Abs. 1 S. 1 RStV weist ausdrücklich darauf hin, dass es sich um ein „an die Allgemeinheit“ gerichtetes Angebot handeln muss.[1106] § 2 Abs. 3 Nr. 1 RStV konkretisiert, dass Rundfunk grundsätzlich nur solche Angebote umfasst, die mehr als 500 potentiellen Nutzern zum zeitgleichen Empfang angeboten werden. Auch systematisch folgt die Notwendigkeit einer gewissen Öffentlichkeit aus dem Schutzzweck der erlassenen Regelungen. Insbesondere das Recht auf eine Gegendarstellung gemäß § 56 RStV und die in § 58 RStV enthaltene Regulierung von Werbung ergeben nur Sinn in einem an die Öffentlichkeit

[1101] *Simitis*, in: Simitis, BDSG, § 1 Rn. 27 m.w.N.
[1102] *Dammann*, in: Simitis, BDSG, § 1 Rn. 149 m.w.N.
[1103] *Micklitz/Schirmbacher*, in Spindler/Schuster, § 55 RStV, Rn. 7.
[1104] *Micklitz/Schirmbacher*, in Spindler/Schuster, § 55 RStV, Rn. 12.
[1105] Vgl. LT-BW-Drs. 14/558, S. 38 f.; siehe auch *Micklitz/Schirmbacher*, in: Spindler/Schuster, § 55 RStV, Rn. 11 ff.
[1106] *Oster*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 4, Rn. 26.

gerichteten Angebot. Es ist daher davon auszugehen, dass Telemedien im Sinne des RStV – und damit auch die von der Ausnahme des § 55 Abs. 1 RStV erfassten Angebote – sich immer an ein potentielles Publikum richten, das über den von § 1 Abs. 2 Nr. 3 BDSG umfassten Kreis deutlich hinausgeht. Ein völliger Gleichlauf der *prima facie* identischen Begriffe ist entsprechend nicht sinnvoll, da es ansonsten für die Ausnahme des § 55 Abs. 1 RStV keinen praktischen Anwendungsbereich mehr gäbe. Sie wäre vielmehr vollkommen unnötig, da sie sich auf einen Sachverhalt beziehen würde, der bereits qua definitionem nicht dem Anwendungsbereich des RStV unterfallen würde.

Anstatt anhand des potentiellen Verbreitungsgrads abzugrenzen – wie bei § 1 Abs. 2 Nr. 3 BDSG –, ist daher im Rahmen des § 55 Abs. 1 RStV auf die individuelle, objektiv erkennbare Zwecksetzung eines Angebots abzustellen. Soweit ein persönliches Profil in sozialen Netzwerken ausschließlich der privaten Kommunikation mit Bekannten dient sowie der digitalen Selbstinszenierung in diesem Kreis, unterfällt es daher der Ausnahmeregelung der persönlichen und familiären Tätigkeit gemäß § 55 Abs. 1 RStV, so dass es keiner Impressumspflicht unterliegt.[1107] Auch wenn sich die private Interaktion auf Personen erstreckt, zu denen keine direkte persönliche Bekanntschaft besteht – wie dies bei Facebook-„Freundschaften“ häufiger der Fall sein kann –, ist die telemedienrechtliche Wahrung der Interessen der Beteiligten sichergestellt, indem der Anbieter des sozialen Netzwerks als Plattformanbieter rechtlich verantwortlich ist.[1108] Sollte sich die Notwendigkeit einer Identifizierung über den Plattformanbieter ergeben, kann diese entweder über die bei der Registrierung hinterlegten Daten oder aber über ein Auskunftsersuchen an den Access-Provider über die IP-Adresse erfolgen.

Dieses Ergebnis wird ferner durch die Vorschrift des § 13 Abs. 6 TMG gestützt, welcher ein Recht auf anonyme oder jedenfalls pseudonyme Nutzung von Telemedien statuiert. Im Rahmen der Dreiecksbeziehung, die sich dadurch ergibt, dass Nutzer auch zugleich Diensteanbieter sein können, kommt es zwingend zu Konflikten mit den Impressumsvorschriften. Es liegt auf der Hand, dass es nachgerade absurd wäre, ein Recht auf anonyme oder pseudonyme Nutzung zu bejahen und gleichzeitig Nutzer nach § 55 Abs. 1 RStV zu verpflichten, ihren Klarnamen und

---

[1107] *Micklitz/Schirmbacher*, in Spindler/Schuster, § 55 RStV, Rn. 13; vgl. auch *Solmecke*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht, Teil 21.1, Rn. 5; a.A. *Ott*, MMR 2007, 354 (356), der einen zusätzlichen Passwortschutz verlangt, wenn die präsentierten Inhalte über den engsten persönlichen Lebens- und Bekanntenkreis hinausgehen.

[1108] a.A. *Richter*, MMR 2014, 517 (519), soweit bei der Registrierung keine Verifizierung der persönlichen Daten erfolgt.

ihre Adresse in ihrem Profil öffentlich zu machen.[1109] Eine solche Auslegung würde vielmehr eine faktische Aufhebung des § 13 Abs. 6 TMG im Kontext sozialer Netzwerke und vergleichbarer Angebote bedeuten. Im Folgenden soll gezeigt werden, dass es möglich ist, diese zunächst in einem Zielkonflikt stehenden Vorschriften miteinander in Einklang zu bringen, indem zwischen einem Recht auf anonyme bzw. pseudonyme Nutzung gegenüber anderen Nutzern sowie gegenüber dem Anbieter des sozialen Netzwerks differenziert wird.

2. Recht auf anonyme oder pseudonyme Nutzung gemäß § 13 Abs. 6 TMG

Grundrechtlich lässt sich ein Recht auf Anonymität aus dem Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG herleiten; Wie jedes andere Recht unterliegt es freilich gewissen Schranken.[1110] Auf einfachgesetzlicher Ebene verpflichtet § 13 Abs. 6 TMG Diensteanbieter, eine anonyme oder pseudonyme Nutzung ihrer angebotenen Telemedien zu ermöglichen, sofern dies technisch möglich und zumutbar ist. Wie oben bereits ausführlich dargelegt wurde, ist spätestens seit dem EuGH-Urteil zu *Google-Spain* im Mai 2014 davon auszugehen, dass entgegen mehrerer instanzgerichtlicher Urteile[1111] dieses Recht auf anonyme bzw. pseudonyme Nutzung für Nutzer von Facebook in Deutschland gilt.[1112]

Dessen ungeachtet statuiert Facebook nach wie vor einen „Klarnamenzwang“ in seinen Nutzungsbedingungen, in denen es unverändert unter Punkt 4 heißt:

> *„Facebook-Nutzer geben ihre wahren Namen und Daten an, und wir benötigen deine Hilfe, damit dies so bleibt. […] 1. Du wirst keine falschen persönlichen Informationen auf Facebook bereitstellen oder ohne Erlaubnis kein Profil für jemand anderen erstellen. 2. Du wirst nur ein einziges persönliches Konto erstellen. […] 10. Wenn du einen Nutzernamen bzw. eine ähnliche Kennung für dein Konto oder deine Seite auswählst, behalten wir uns das Recht vor, diese/n zu entfernen oder zu widerrufen, sollten wir dies als notwendig erachten.“*[1113]

[1109] *Richter*, MMR 2014, 517 (519 f.); vgl. auch *Stadler*, ZD 2011, 57 (58 f.).

[1110] ausführlich: *Nietsch*, Anonymität, S. 38 ff.; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 33 ff.; *ders./Nink*, in: Spindler/Schuster, § 13 TMG Rn. 21; *Scholz*, in: Simitis, BDSG, § 3a, Rn. 19.

[1111] VG Schleswig, ZD 2013, 245 (245 f.); OVG Schleswig, ZD 2013, 364 (365); VG Hamburg, ZD 2016, 243 (244 ff.).

[1112] Vgl. zur Anwendbarkeit deutschen Datenschutzrechts ausführlich oben unter C.II.4.b).

[1113] https://www.facebook.com/legal/terms?ref=pf (Stand 30. Januar 2015); auch andere soziale Netzwerke wie beispielsweise LinkedIn statuieren einen solchen Klarnamenzwang, vgl. dort Punkt 8 der Nutzungsbedingungen, https://www.linkedin.com/legal/user-agreement?trk=uno-reg-guest-home-user-agreement (Stand 7. Juni 2017).

Der Klarnamenzwang wird durchgesetzt, indem Benutzerkonten, bei denen Facebook annimmt, dass kein Klarname verwendet wurde, gesperrt und nur dann wieder freigeschaltet werden, wenn eine Kopie eines Personalausweises oder eines vergleichbaren amtlichen Identifizierungsdokumentes übersandt wird.[1114] Der Klarnamenzwang gilt nicht nur für die bei der Registrierung gemachten Angaben, sondern auch für die den anderen Nutzern angezeigten Profilnamen. Im Juli 2015 wurde deshalb vom Hamburgischen Beauftragten für Datenschutz und Informationssicherheit eine Anordnung gemäß § 38 Abs. 5 BDSG erlassen, die Facebook aufgab, zukünftig eine pseudonyme Nutzung zumindest gegenüber anderen Nutzern zuzulassen.[1115] Allerdings ist Facebook hiergegen vorerst erfolgreich gerichtlich vorgegangen, indem das *VG Hamburg* Facebooks Klage im einstweiligen Rechtsschutz gegen die ebenfalls angeordnete sofortige Vollziehbarkeit stattgegeben und die aufschiebende Wirkung des gegen den Bescheid eingelegten Widerspruchs wiederhergestellt hat. Begründet wurde dies – nach hier vertretener Ansicht unzutreffend – mit einer mangelnden Anwendbarkeit des deutschen Datenschutzrechts.[1116]

Die Anordnung des hamburgischen Datenschutzbeauftragten ist trotz der gerichtlichen Niederlage im erstinstanzlichen einstweiligen Rechtsschutz sehr zu begrüßen, da es sich bei dem Klarnamenzwang um einen erheblichen Eingriff in die informationelle Selbstbestimmung der Nutzer handelt. Die Möglichkeit, sich pseudonym im Internet zu bewegen und zu präsentieren ist letztlich eine Voraussetzung dafür, seine Persönlichkeit frei entfalten zu können.[1117] Zudem stellt § 13 Abs. 6 TMG eine Konkretisierung des Datenvermeidungsgebots aus § 3a BDSG dar und setzt damit ein Kernelement des Datenschutzes im Zeitalter ubiquitärer Datenverarbeitung um.[1118] Das Recht auf anonyme bzw. pseudonyme Nutzung ist daher gerade auch im Zusammenhang mit sozialen Netzwerken von besonderer Bedeutung. Zu klären ist indes, in welchem Umfang dieses Recht zu gewähren ist: Denkbar ist einerseits, dass es nur die Pseudonymität bei der Interaktion mit anderen Nutzern umfasst, jedoch kein Recht auf Anonymität gegenüber dem Anbieter gewährt. Andererseits könnte man aber auch annehmen, dass es noch weiter geht und Nutzer auch Anbietern wie Facebook ihren Klarnamen nicht

---

1114 *Ziebarth*, ZD 2013, 375 (376); *Schnabel/Freund*, CR 2010, 718 (720).

1115 https://www.datenschutz-hamburg.de/news/detail/article/der-hamburgische-datenschutzbeauftragte-profilnamen-bei-facebook-frei-waehlbar.html?tx_ttnews[backPid]=1&cHash=c2a6cea29f0fd07dae7ca92f86c724cc.

1116 VG Hamburg, ZD 2016, 243 (244 ff.). Das OVG Hamburg, ZD 2016, 450 (451 ff.), hat in zweiter Instanz ebenfalls den Eilrechtsschutz verneint, für die materiellrechtliche Klärung aber auf das durch das BVerwG angestrengte Vorabentscheidungsverfahren durch den EuGH verwiesen (ZD 2016, 393 (393 ff.)).

1117 Vgl. *Caspar*, ZRP 2015, 233 (235); *Härting*, NJW 2013, 2065 (2068); *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 148.

1118 *Caspar*, ZRP 2015, 233 (235); *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 21; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 148 f.

offenbaren müssen. Vorab ist allerdings zu untersuchen, ob dieses Recht mit Anwendbarkeit der DS-GVO überhaupt noch Bestand haben wird.

a) Auswirkungen der DS-GVO

Die DS-GVO enthält – ebenso wie früher die DSRL – kein direkt mit § 13 Abs. 6 TMG vergleichbares Recht. Da § 13 Abs. 6 TMG und seine Vorgängervorschrift § 4 TDDSG nicht auf die DSRL für elektronische Kommunikation zurückgehen, sondern eine überschießende Umsetzung der allgemeinen DSRL darstellen[1119], spricht zunächst vieles dafür, dass die Norm durch die DS-GVO verdrängt und unanwendbar wird.[1120]

Das Konzept einer pseudonymen Nutzung ist der DS-GVO allerdings nicht fremd. Sie verweist an verschiedenen Stellen darauf, dass eine schnelle Pseudonymisierung von Daten zur Erhöhung der Datensicherheit empfehlenswert ist, beispielsweise in den Erwägungsgründen 28 und 78. Art. 25 und 32 DS-GVO fordern Datenverarbeiter ausdrücklich dazu auf, technische Datensicherheits-Maßnahmen wie eine Pseudonymisierung zu implementieren, sofern dies mit vertretbarem Aufwand möglich ist und dem Verarbeitungszweck nicht widerspricht. Dies kann jedenfalls für die Frage der pseudonymen Nutzung gegenüber anderen Nutzern in sozialen Netzwerken bejaht werden, wie die nachfolgende Argumentation sogleich unter b) zeigen wird. Angesichts der besonderen Bedeutung der pseudonymen Nutzungsmöglichkeit für den Selbstdatenschutz[1121] wäre es jedenfalls zu begrüßen, wenn die zukünftige Rechtspraxis einen entsprechenden Anspruch auf pseudonyme Nutzung aus den Normen bestätigt.

Ein Recht auf pseudonyme Nutzung könnte sich auch aus Art. 5 Abs. 1 lit. b) und c) DS-GVO herleiten lassen. Diese übernehmen weitgehend die in Art. 6 Abs. 1 lit. c) DSRL normierten Grundsätzen der Zweckbindung und der Datenvermeidung, welche bisher als Aufforderung zu

---

[1119] *Schaar/Schulz*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, § 4 TDDSG, Rn. 24 ff.

[1120] Etwas anderes würde dann gelten, sofern den Mitgliedstaaten ein Umsetzungsspielraum für derartige Regelungen verbleibt. Ein solcher könnte sich aus Erwägungsgrund 10 DS-GVO ergeben, wonach den Mitgliedstaaten ein Umsetzungsspielraum in Bezug auf die Verarbeitung sensibler Daten verbleibt. Diese Regelung ist vergleichbar zu dem früheren Erwägungsgrund 53 DSRL, wonach Mitgliedstaaten für besonders gefährdete Daten eigene, spezifischere Regeln erlassen durften. Hierauf basierte maßgeblich der frühere § 4 TDDSG, vgl. *Schaar/Schulz*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, § 4 TDDSG, Rn. 24 ff. Ein Umsetzungsspielraum könnte weiterhin aus Art. 85 Abs. 1 DS-GVO folgen, wonach die Mitgliedstaaten das Datenschutzrecht mit dem Recht auf Meinungs- und Informationsfreiheit durch Gesetz in Einklang bringen sollen. Wie nachfolgend zu zeigen sein wird, kann ein Klarnamenzwang einen erheblichen negativen Einfluss auf die freie Meinungsäußerung von Nutzern in sozialen Netzwerken haben. Es scheint daher jedenfalls denkbar, dass eine derartige Regelung zulässig wäre. Ob dies der Fall ist, kann indes letztlich nur durch den EuGH entschieden werden. Angesichts des vollharmonisierenden Anspruchs der DS-GVO erscheint eine Verdrängung aber wahrscheinlicher.

[1121] Hierzu ausführlich unten unter D.III.3.a).

pseudonymen Nutzungsmöglichkeiten interpretiert wurden: Insbesondere Anbieter von sozialen Netzwerken sollten „sorgfältig abwägen", ob sie ihre Nutzer zur Angabe ihre wahren Namens anstelle eines Pseudonyms zwingen können.[1122]

Zuletzt können sowohl das in Art. 7 GrCH statuierte Recht auf Achtung des Privatlebens und der Kommunikation als auch das Recht auf den Schutz personenbezogener Daten aus Art. 8 GrCH als grundrechtliche Ansatzpunkte für ein Recht auf Anonymität herangezogen werden.[1123]

Unabhängig davon, ob § 13 Abs. 6 TMG unter Geltung der DS-GVO unanwendbar wird, wird sich somit die Frage nach der Notwendigkeit einer pseudonymen Nutzungsmöglichkeit gegenüber anderen Nutzern weiterhin stellen. Die aktuell noch relevante Frage nach einer anonymen Nutzungsmöglichkeit gegenüber dem Anbieter wird sich dagegen erledigen, sofern § 13 Abs. 6 TMG nicht als zulässige mitgliedstaatliche Konkretisierung anwendbar bleiben sollte, da ein derart weitgehendes Recht nicht aus der DS-GVO ableitbar scheint.

b) Schutz gegenüber anderen Nutzern

Gegen ein Recht der Nutzer auf pseudonyme Nutzung untereinander wird vor allem vorgebracht, dass dies den Anbietern sozialer Netzwerke unzumutbar sei: Eine pseudonyme Nutzung schränke die Möglichkeit der Vernetzung der Nutzer untereinander ein fördere und zudem Beleidigungen und andere Rechtsverletzungen.[1124] Hierdurch würden der wirtschaftliche Erfolg und die gesellschaftliche Bedeutung sozialer Netzwerke negativ beeinflusst, da das Vernetzungspotential eingeschränkt werde.[1125] Während diese Argumente durchaus ihre Berechtigung haben – insbesondere die jüngste erfolgte Verabschiedung des Netzwerkdurchsetzungsgesetzes (NetzDG) unterstreicht die praktische Relevanz des Problems

[1122] Art. 29 DatSchGruppe, Stellungnahme 5/2009, WP 163, S. 13; lediglich von einem „Anreiz an die datenverarbeitenden Stellen, Daten anonymisiert zu verarbeiten" bzw. eine „Wertung zugunsten der Nutzung anonymer Daten" spricht *Nietsch*, Anonymität, S. 34 f., 37; vgl. auch *Caspar*, ZRP 2015, 233 (234); *Schantz*, NJW 2016, 1841 (1841 f.).

[1123] *Nietsch*, Anonymität, S. 32 f.; vgl. auch *Skouris*, NVwZ 2016, 1359 (1361), welcher zumindest das Recht auf Vergessenwerden aus den Art. 7 und 8 GrCH ableitet.

[1124] So *Bender*, K&R 2013, 218 (219).

[1125] *Bender*, K&R 2013, 218 (219).

der Verbreitung rechtswidriger Inhalte in sozialen Netzwerken[1126] –, können sie doch im Ergebnis nicht überzeugen.[1127]

aa) Zuverlässige Identifizierung anderer Nutzer

Zunächst entspricht es gerade der eindeutigen gesetzgeberischen Wertentscheidung in § 13 Abs. 6 TMG, dass es keinen Anspruch der anderen Nutzer gibt, über die Identität ihres jeweiligen Gegenübers aufgeklärt zu werden.[1128] Wer in einem sozialen Netzwerk unter seinem Klarnamen gefunden werden will und ein entsprechendes Interesse an Vernetzung zeigt, kann sein Profil entsprechend gestalten. Eine Pflicht zur Preisgabe der eigenen Identität untergräbt dagegen die datenschutzrechtlichen Selbstschutzmöglichkeiten eines Nutzers erheblich und verfehlt die staatliche Pflicht, einen sicheren Kommunikationsraum zu gewährleisten.[1129] Auch bei sozialen Netzwerken, die kostenpflichtig zur Vernetzung im Beruf angeboten werden, wie etwa LinkedIn[1130], muss diese Abwägung letztendlich zugunsten der informationellen Selbstbestimmung der Nutzer ausfallen. Freilich lässt sich argumentieren, dass es in diesen Netzwerken noch von viel größerer Bedeutung ist, die Identität seines Kontaktes zu kennen, um sich sinnvoll mit ihm vernetzen zu können.[1131] Dies zäumt das Pferd indes von hinten auf: Eine Anmeldung bei LinkedIn garantiert mitnichten eine erfolgreiche Vermittlung von verifizierten Kontakten. Sie bietet dem Anmeldenden vielmehr nur eine Chance, sich selbst zu präsentieren und von anderen kontaktiert zu werden bzw. sich selbst als Kontakt anzubieten. Den Dienst pseudonym, wenn nicht gar anonym zu nutzen, bedeutet für den Nutzer auch eine Verringerung seiner eigenen Kontaktchancen, da er im Zweifel seltener gefunden werden kann. Es sollte dem Nutzer freistehen, diesen Nachteil zur Wahrung seiner Anonymität

---

[1126] Instruktiv aber sehr kritisch zum NetzDG, jeweils m.w.N.: *Guggenberger*, NJW 2017, 2577 (2577 ff.); *Kalscheuer/Hornung*, NVwZ 2017, 1721 (1722 ff.); positiv dagegen *Schwartmann*, GRUR-Prax, 2017, 317 (317 ff.)

[1127] Vgl. auch *Hullen/Roggenkamp*, in: Plath, § 13 TMG, Rn. 42; *Moos*, in: Taeger/Gabel, § 13 TMG, Rn. 48; *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 23 ff.; im Ergebnis so wohl auch *Maisch*, Informationelle Selbstbestimmung, S. 192 ff.

[1128] Vgl. BT-Drs. 13/7385, S. 71.

[1129] *Caspar*, ZRP 2015, 233 (235 f.); *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 21 f.; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 148 ff.; vgl. auch *Moos*, in: Taeger/Gabel, § 13 TMG, Rn. 48; *Nietsch*, Anonymität, S. 50 f.; vgl. zur staatlichen Schutzpflicht auch BVerfG 65, 1 (44) – Volkszählung; BVerfGE 120, 274 (306) – Onlinedurchsuchung; zur Bedeutung des Selbstdatenschutzes in sozialen Netzwerken auch noch ausführlich unten unter D.III.3.a).

[1130] LinkedIn statuiert in Punkt 8 seiner Nutzungsbedingungen einen ausdrücklichen Klarnamenzwang sowohl bei der Registrierung als auch in der Benennung des Profils gegenüber anderen Nutzern, vgl. https://www.linkedin.com/legal/user-agreement?trk=uno-reg-guest-home-user-agreement (Stand 7. Juni 2017).

[1131] In diese Richtung *Hullen/Roggenkamp*, in: Plath, § 13 TMG, Rn. 42 m.w.N.; *Moos*, in: Taeger/Gabel, § 13 TMG, Rn. 52.

inkaufzunehmen. Auch in einem direkten Gespräch etwa auf einer Karrieremesse gibt es keine Pflicht eines Teilnehmers, sich einem anderen gegenüber mit seinem Personalausweis und damit seinem Klarnamen auszuweisen. In der Abwägung zwischen dem Interesse an pseudonymer Nutzung zum Schutz der informationellen Selbstbestimmung und dem Interesse der anderen Nutzer an der wahren Identität wiegt ersteres schwerer: Kein Nutzer hat einen Anspruch darauf, die wahre Identität des anderen zu erfahren.

Zudem ist es der Kommunikation im Internet immanent, dass man keine letztgültige Sicherheit über die Identität des Kommunikationspartners haben kann.[1132] Vielmehr empfiehlt es sich, hier grundsätzlich ein gesundes Maß an Vorsicht walten zu lassen, insbesondere auch mit Blick auf Phishing-Mails oder Fake-Profile potentieller Straftäter. Ein vertraglich statuierter Klarnamenzwang in sozialen Netzwerken kann diesen Gefahren nicht wirksam begegnen, da eine zu große Umgehungsgefahr entstünde: Da eine Überprüfung der Personalien nicht *ex ante* stattfindet, sondern nur *ex post*, wenn ein Verdacht auf einen konkreten Missbrauch besteht, können zunächst gefälschte Profile eingerichtet werden. Zu suggerieren, dass Personen in sozialen Netzwerken stets unter ihrem Klarnamen auftreten, schafft ein falsches Gefühl der Sicherheit und ist daher der Sicherheit sogar eher abträglich.[1133] Dies gilt in gleichem Maße für Karrierenetzwerke wie LinkedIn, in denen bei einer Vereinbarung möglicher Bewerbungsgespräche oder Absprachen über Gehälter eine Sicherheit bezüglich der Identität des Gesprächspartners zwar suggeriert, aber letztendlich nicht gewährleistet werden kann.

bb) Rechtsdurchsetzung und Ahndung von Rechtsverstößen

Auch der Ruf nach wirksamer Strafverfolgung und „einem gesteigerten Maß an sozialer Kontrolle“[1134] durch den Klarnamenzwang erweisen sich letztlich nicht als überzeugende Argumente. Die effektive Strafverfolgung ist nicht davon abhängig, unter welchem Namen eine Person sich im sozialen Netzwerk präsentiert, da einerseits auf die Registrierungsdaten

[1132] Entsprechend besteht regelmäßig auch kein schutzwürdiges Vertrauen in die Identität eines Kommunikationspartners, vgl. BVerfGE 120, 274, 345 – Onlinedurchsuchung = NJW 2008, 822, 836 Rn. 311.

[1133] So auch *Caspar*, ZRP 2015, 233 (236); A.A. *Bender*, K&R 2013, 218 (219); *Irish Data Protection Commissioner*, Report of Audit, 21.12.2011, S. 137.

[1134] *Bender*, K&R 2013, 218 (219); vgl. auch *Heckmann*, NJW 2012, 2631 (2632); *Kutscha*, GR-Schutz im Internet, S. 50; *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 78 f.

zurückgegriffen werden kann, andererseits auf die IP-Adresse.[1135] Zudem mag es zwar auf den ersten Blick einleuchtend klingen, dass ein Auftritt unter Klarnamen zu einem freundlicheren und respektvolleren Umgang der Nutzer untereinander führt.[1136] Die Realität zeigt jedoch in zahlreichen sozialen Netzwerken, dass Ausfälle und Beschimpfungen bis hin zu strafrechtlich relevanten Beleidigungen und sogar Volksverhetzung auch bei der Nutzung von Klarnamen auftreten.[1137] Die bloße Möglichkeit, dass solche Straftaten unter einer Klarnamenpflicht seltener auftreten könnten, wiegt angesichts der möglichen Schäden, die mit einer Klarnamenpflicht einhergehen, nicht schwer genug um sie zu rechtfertigen.[1138]

Der BGH hat darüber hinaus mit Urteil vom 1.7.2014 entschieden, dass im Falle von Persönlichkeitsrechtsverletzungen kein Anspruch des Geschädigten gegenüber dem Diensteanbieter auf die Herausgabe von Nutzerdaten existiert, insbesondere auch nicht aus § 242 BGB.[1139] Während sich grundsätzlich Auskunftsansprüche zur Durchsetzung eigener Rechte aus Treu und Glauben ergeben könnten, scheitere ein solcher Anspruch in diesem Kontext daran, dass es für den Diensteanbieter keine datenschutzrechtliche Ermächtigung für die Herausgabe dieser Daten ohne eine Einwilligung des Betroffenen gebe. Eine solche Übermittlung sei nicht von § 12 Abs. 2 TMG erfasst und der Auskunftsanspruch aus § 242 BGB nicht ausdrücklich auf Telemedien bezogen.[1140] Eine analoge Anwendung der §§ 14 Abs. 2, 15 Abs. 5 TMG, die eine entsprechende Herausgabe an die zuständigen staatlichen Stellen u.a. zu Zwecken der Strafverfolgung gestatten, scheitere an einer planwidrigen Regelungslücke.[1141] Die Erteilung der Auskunft an Private sei daher rechtlich unmöglich und könne entsprechend nicht verlangt werden.[1142] Die Frage, ob darüber hinaus auch § 13 Abs. 6 TMG einer solchen Auskunftserteilung entgegensteht, hat der BGH mangels Entscheidungsrelevanz ausdrücklich

---

[1135] Ausführlich zu den technischen Grundlagen *Nietsch*, Anonymität, S. 60 ff.; vgl. auch *Klar*, DÖV 2013, 103 (109); BT-Drs. 13/7385. Natürlich besteht das Risiko, dass beispielsweise die IP-Adresse verschleiert wird oder anderweitig nicht eindeutig zugeordnet werden kann, indem beispielsweise mehrere Leute dieselbe Adresse verwenden, vgl. *Heckmann*, NJW 2012, 2631 (2634 f.). Auch hier hilft ein Klarnamenzwang indes nur begrenzt weiter: Wer bewusst seine IP-Adresse verschleiert, um online Straftaten zu begehen, wird sich von einem solchen Klarnamenzwang im Zweifel nicht beeindrucken lassen, sondern einen falschen Namen angeben. Dem Problem der Nutzung eines Internetanschlusses durch verschiedene Personen lässt sich zudem durch einen Rückgriff auf die Login-Daten des spezifischen Accounts lösen, mit dem die Rechtsverletzung verübt wurde. Diese liegen dem Anbieter des sozialen Netzwerks stets vor. Zudem besteht auch im Rahmen mancher Anonymisierungsdiente die Möglichkeit einer späteren Reidentifizierung trotz der zunächst verschleierten IP-Adresse; dazu ausführlich *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 23 ff.

[1136] Vgl. *Heckmann*, NJW 2012, 2631 (2632); *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 78.

[1137] So auch *Caspar*, ZRP 2015, 233 (235).

[1138] So auch *Heckmann*, NJW 2012, 2631 (2632 f.); *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 84 f.

[1139] BGH, BGHZ 201, 380 (384), Rn. 11.

[1140] BGH, BGHZ 201, 380 (383), Rn. 9.

[1141] BGH, BGHZ 201, 380 (385 f.), Rn. 13 ff.

[1142] BGH, BGHZ 201, 380 (383), Rn. 9; so auch *Lauber-Rönsberg*, MMR 2014, 10 (13 f.).

offen gelassen.[1143] In der instanzgerichtlichen Rechtsprechung wird sie verbreitet bejaht.[1144] Dem ist *de lege lata* im Ergebnis wohl zuzustimmen: Die eng begrenzten gesetzlichen Ermächtigungen zur Übermittlung der Daten gemäß §§ 14 Abs. 2, 15 Abs. 5 TMG stellen eine systematische Beschränkung des Rechts auf anonyme Nutzung aus § 13 Abs. 6 TMG dar und zeigen eine gesetzgeberische Wertentscheidung, dass das Recht auf anonyme Nutzung nur unter den dort genannten Voraussetzungen gegenüber dem Interesse an einer wirksamen Rechtsdurchsetzung und Strafverfolgung zurückzutreten hat.[1145] Da es keine gesetzliche Erlaubnis dafür gibt, die entsprechenden Daten an Geschädigte einer Persönlichkeitsrechtsverletzung herauszugeben, zeigt sich im Umkehrschluss, dass der Gesetzgeber insoweit keine Einschränkung des Rechts auf anonyme Nutzung bezweckt hat. Der Gesetzgeber billigt damit die Konsequenz, dass unter dem Deckmantel der Anonymität Persönlichkeitsrechtsverletzungen begangen werden können, die keine rechtlichen Konsequenzen nach sich ziehen, sofern sie unterhalb einer strafrechtlich relevanten Schwelle bleiben. Selbst wenn der Verdacht auf Beleidigungen gemäß §§ 185 ff. StGB besteht, kann die Staatsanwaltschaft in Ermangelung eines öffentlichen Interesses auf den Privatklageweg nach § 374 Abs. 1 Nr. 2 StPO verweisen.[1146] Eine effektive Rechtsdurchsetzung wird dem Privaten damit in vielen Fällen faktisch unmöglich gemacht. Da entsprechende Persönlichkeitsrechtsverletzungen weder eine schützenswerte Ausübung des Rechts auf freie Persönlichkeitsentfaltung noch auf freie Meinungsäußerung sind, die der Regelung des § 13 Abs. 6 TMG zugrunde liegen, wäre es daher *de lege ferenda* wünschenswert, wenn ein entsprechender Auskunftsanspruch Privater – freilich nur unter strengen Voraussetzungen – gewährt würde.[1147]

[1143] BGH, BGHZ 201, 380 (383), Rn. 8

[1144] LG München I, CR 2013, 677 (678); OLG Hamm, CR 2012, 128 (128); KG Berlin, MMR 2007, 116 (117); a.A. OLG Dresden, K&R 2012, 626 (628).

[1145] So im Ergebnis auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 58.

[1146] *Krohm/Müller-Peltzer*, ZD 2015, 409 (412).

[1147] So auch *Krohm/Müller-Peltzer*, ZD 2015, 409 (412); *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 111 f.; vgl. auch den BGH, BGHZ 201, 380 (386), Rn. 17. Die Bundesregierung hatte insoweit im Rahmen des Gesetzgebungsverfahrens zur Verbandsklage im Datenschutz zugesagt, die Notwendigkeit einer Erweiterung der Auskunftsrechte von Diensteanbietern eingehend zu erörtern und zu prüfen, BT-Drs. 18/4631, S. 39. Nach Angaben des AK Vorratsdatenspeicherung vom 14.12.2015 unter Verweis auf Informationen aus Reihen der Koalition im Vorfeld der Bundestagsanhörung zur WLAN-Haftung wurde diese Erweiterung indes vorerst verworfen und war nicht Gegenstand der aktuellen Reform des Telemediengesetzes, http://www.vorratsdatenspeicherung.de/content/view/766/79/lang,de/.

cc) Schutz der Meinungs- und persönlichen Entfaltungsfreiheit

Eine Klarnamenpflicht gegenüber anderen Nutzern schränkt das Recht auf freie Entfaltung der Persönlichkeit ein und kann durch eine abschreckende Wirkung auch die Meinungsfreiheit negativ berühren: Wer sich in einem öffentlich einsehbaren Forum stets mit seinem Klarnamen gegenüber einer unbekannten Anzahl von Adressaten äußern muss, kann hierdurch eingeschüchtert werden und entsprechend auf eine Äußerung verzichten.[1148] Selbst wenn die Sichtbarkeit der eigenen Beiträge auf engere Freunde und Bekannte beschränkt wird, können diese die Beiträge mit wenigen Klicks weiterverbreiten, ohne dass der Äußernde dies effektiv kontrollieren und verhindern kann. Dies betrifft keinesfalls nur extreme, möglicherweise rechtswidrige Äußerungen, deren Schutz im Rahmen der Meinungsfreiheit zweifelhaft wäre. Vielmehr lässt sich im Internet häufig das Phänomen des „Shitstorms" beobachten, bei dem auf Personen wegen ihrer Meinungsäußerung eine virtuelle Hexenjagd veranstaltet wird, ohne dass diese Meinungsäußerung irgendeine strafrechtliche Relevanz aufweist.[1149] Durch die langfristige Speicherung von Aussagen im Internet im Allgemeinen und sozialen Netzwerken im Besonderen muss zudem stets damit gerechnet werden, dass eine frühere Äußerung aus dem Kontext gerissen wird und dann zu nachteiligen Folgen führt.[1150] Auch niederschwelliger können sich Abschreckungseffekte ergeben, wenn beispielsweise Aussagen unter Klarnamen getätigt werden müssen, die im unmittelbaren sozialen Umfeld des Sich-Äußernden zu Ablehnung oder Ächtung führen.[1151]

In solchen Fällen wird zudem die persönliche Entfaltungsfreiheit erheblich eingeschränkt, wenn entsprechende persönliche Ansichten und Einstellungen bei der Profilgestaltung konsequent verborgen werden müssen, um zu verhindern, dass negative soziale Konsequenzen eintreten. Angesichts der erheblichen gesellschaftlichen Bedeutung und Verbreitung, die soziale Netzwerke insbesondere in jüngeren Generationen mittlerweile haben[1152], kann dies eine sehr einschneidende Beschränkung sein. Zur Gewährleistung einer freien Meinungsäußerung und

---

[1148] *Krohm/Müller-Peltzer*, ZD 2015, 409 (415); *Caspar*, ZRP 2015, 233 (235); *Nietsch*, Anonymität, S. 47 f.; *Oermann/Staben*, Der Staat (52) 2013, S. 648 f. m.w.N.; *Heckmann*, NJW 2012, 2631 (2632); *Das/Kramer*, Self-Censorship on Facebook, http://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350, S. 120, 125; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 25; vgl. auch *Mayer-Schönberger*, Die Tugend des Vergessens, S. 131 f.

[1149] *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 318 f.

[1150] *Mayer*-Schönberger, Die Tugend des Vergessens, S. 131 f.

[1151] *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 25 f.; *Mayer*-Schönberger, Die Tugend des Vergessens, S. 131 f. Denkbare Fälle hierfür sind z.B. eine vom sozialen Umfeld nicht tolerierte politische Einstellung oder sexuelle Orientierung.

[1152] Hierzu bereits oben unter B.I.2.

Persönlichkeitsentfaltung auch in sozialen Netzwerken besteht daher eine staatliche Schutzpflicht, eine pseudonyme Nutzung zu ermöglichen.

dd) Sonderfall: Diensteanbietende Nutzer

Eine Ausnahme besteht lediglich dann, wenn Nutzer selbst als Diensteanbieter im Sinne von § 2 Nr. 1 TMG einzustufen sind, etwa weil sie das soziale Netzwerk zu kommerziellen Zwecken nutzen.[1153] In diesem Fall unterliegen sie eigenen telemedienrechtlichen Pflichten, insbesondere der Impressumspflicht gemäß § 5 Abs. 1 TMG. Die hieraus folgende Beschränkung der Rechte aus § 13 Abs. 6 TMG ist systematisch im TMG angelegt, welches von einem dichotomen Verhältnis von Nutzern und Diensteanbietern ausgeht. Nutzer, die ihre Profile in sozialen Netzwerken nicht ausschließlich privat nutzen, nehmen hier eine im Gesetz nicht ausdrücklich geregelte, aber logisch ableitbare Doppelnatur ein: Gegenüber dem Anbieter des sozialen Netzwerks sind sie als Nutzer einzustufen; gegenüber weiteren Nutzern dagegen als Diensteanbieter. Diese Doppelnatur als „diensteanbietender Nutzer“ führt freilich zu einem exklusiven Verhältnis der Rechte und Pflichten aus dem TMG: Wird eine Impressumspflicht bejaht, ist eine anonyme Nutzung nicht mehr möglich. Diese Konkurrenz ist durch eine Abwägung aufzulösen, welcher Aspekt der Doppelnatur insgesamt schwerer wiegt. Diese Abwägung fällt zugunsten der Natur als Diensteanbieter aus: Es liegt in der freien Entscheidung eines Nutzers, sein Profil nicht rein privat zu nutzen, sondern gewerblich. Ein gewerblich ausgerichtetes Profil ist zwingend auch auf die Öffentlichkeit ausgerichtet und darauf, geschäftliche Beziehungen einzugehen. Insoweit erwächst für die anderen, adressierten Nutzer ein Schutzbedürfnis, ihren Geschäftspartner zuverlässig identifizieren zu können. Dieses Schutzbedürfnis wiegt im Ergebnis schwerer als das Interesse des diensteanbietenden Nutzers an einer Geheimhaltung seiner Identität. Er ist daher zur Bereithaltung eines Impressums verpflichtet, ohne dass § 13 Abs. 6 TMG dem entgegenstünde.

Betrachtet man dies sehr spitzfindig, könnte man natürlich sagen, dass die Statuierung eines Klarnamenzwangs für kommerziell genutzte Profile in den Nutzungsbedingungen des sozialen Netzwerks dennoch vertragsrechtlich unzulässig sein kann. Denn der diensteanbietende Nutzer unterfällt grundsätzlich durchaus dem Schutzbereich des § 13 Abs. 6 TMG im Verhältnis zum Diensteanbieter. Er kann dieses Recht lediglich nicht nutzen, da ihn eine konkurrierende, objektiv-rechtliche Pflicht aus § 5 Abs. 1 TMG trifft, das Impressum vorzuhalten. Entsprechend kann es streng genommen allenfalls zulässig sein, in den Nutzungsbedingungen die Pflicht zur

[1153] Zu dieser Abgrenzung bereits ausführlich oben unter D.I.3.b)cc).

Erstellung eines Impressums zu normieren. Dies macht insoweit einen Unterschied, als der Profilname dann nicht zwingend der Klarname sein muss, solange das Impressum mit nicht mehr als zwei Klicks eindeutig und unmittelbar erreichbar ist.[1154]

Abseits der bestehenden Impressumspflicht als „diensteanbietender Nutzer" zeigt die gesetzgeberische Wertentscheidung in § 55 Abs. 1 RStV, dass eine individuelle Identifizierbarkeit durch andere Nutzer nicht zwingend erforderlich ist.[1155] Es ist daher festzuhalten, dass § 13 Abs. 6 TMG das Recht einräumt, privat genutzte Nutzungsprofile jedenfalls gegenüber anderen Nutzern pseudonym zu verwenden. Die Gewährung dieses Rechts ist den Anbietern sozialer Netzwerke auch zuzumuten. Für gewerblich genutzte Profile ist dagegen gemäß § 5 Abs. 1 TMG ein Impressum erforderlich. Auch dies setzt indes nicht zwingend voraus, dass auch das Profil mit Klarnamen benannt wird. Der von Facebook pauschal statuierte Klarnamenzwang für Nutzerprofile ist somit rechtswidrig.[1156]

c) Schutz gegenüber dem Anbieter sozialer Netzwerke

Nicht abschließend geklärt ist, ob das Recht auf anonyme bzw. pseudonyme Nutzung darüber hinaus auch gegenüber dem Anbieter des sozialen Netzwerks selbst besteht. Im Kern geht es hierbei um die Frage, ob eine *anonyme* Registrierung möglich sein muss, da bei einer bloßen Pseudonymisierung dem Anbieter des sozialen Netzwerks die Zuordnung qua definitionem noch möglich wäre, vgl. § 3 Abs. 6, 6a BDSG, und sich somit kein relevanter Gewinn an Privatheit für die Nutzer ergäbe.

Das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein ordnete 2013 in einer Verfügung gemäß § 38 Abs. 5 BDSG an, eine entsprechende anonyme Registrierung zuzulassen. Da die zuständigen Verwaltungsgerichte deutsches Datenschutzrecht – unzutreffenderweise – im einstweiligen Rechtsschutzverfahren für unanwendbar erklärten, wurde diese Verfügung jedoch aufgehoben, ohne dass es zu einer höchstrichtlichen Klärung der zugrunde liegenden Rechtsfrage kam.[1157] Die im Sommer 2015 vom Hamburgischen

---

[1154] Vgl. BGH, NJW 2006, 3633 (3634 f.); instruktiv zum Erfordernis der unmittelbaren Erreichbarkeit des Impressums *Micklitz/Schirmbacher*, in: Spindler/Schuster, § 5 Rn. 36 m.w.N.

[1155] Hierzu ausführlich im vorigen Abschnitt unter D.II.1.

[1156] *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 21 f.; *Ziebarth*, ZD 2013, 375, 376, unter der (zu bejahenden) Prämisse, dass § 13 Abs. 6 TMG kollisionsrechtlich anwendbar sein müsste; *Kremer*, CR 2012, 438 (442); *Stadler*, ZD 2011, 57 (58); *Schnabel/Freund*, CR 2010, 718 (720); vgl. auch *Schreibauer*, in: Auernhammer: § 13 TMG Rn. 54; *Hullen/Roggenkamp*, in: Plath, § 13 TMG, Rn. 42; *Moos*, in: Taeger/Gabel, § 13 TMG, Rn. 48, 52.

[1157] VG Schleswig, ZD 2013, 245 (245 f.); OVG Schleswig, ZD 2013, 364 (364 f).

Beauftragten für Datenschutz und Informationssicherheit gegen Facebook erlassene Verfügung verzichtet dagegen auf die Anordnung der Schaffung einer anonymen Registrierungsmöglichkeit. Stattdessen mahnt sie lediglich die Schaffung einer pseudonymen Nutzungsmöglichkeit gegenüber anderen Nutzern an. Die in den Nutzungsbedingungen Facebooks statuierte Pflicht, bei Zweifeln an der Identität eine Kopie des Personalausweises oder eines vergleichbaren amtlichen Lichtbildausweises einzureichen, wurde allerdings als Verstoß gegen das Pass- und Personalausweisgesetz eingestuft.[1158]

Gegner eines Rechts auf anonyme Registrierung verweisen auf den Wortlaut des § 13 Abs. 6 TMG, der lediglich die *Nutzung* von Telemedien erfasse. Es sei klar ersichtlich, dass nur ein Recht auf eine anonyme bzw. pseudonyme Nutzung im engeren Sinne normiert sei, nicht aber ein Recht auf eine entsprechende Registrierung gegenüber dem Anbieter.[1159] Zudem gehöre der Name zu den *essentialia negotii*, die zwingend bei dem mit der Registrierung verbundenen Vertragsschluss anzugeben sind.[1160] Ein Recht auf eine anonyme Registrierung würde im Umkehrschluss eine Verpflichtung zu anonymen Vertragsschlüssen bedeuten und damit einen unvertretbaren Eingriff in die Vertragsfreiheit der Diensteanbieter.[1161]

In dieser Absolutheit überzeugt diese Ablehnung nicht, da es das Recht auf eine anonyme Nutzung ad absurdum führen würde.[1162] Gemäß der Legaldefinition des § 3 Abs. 6 BDSG bedeutet eine Anonymisierung, dass Einzelangaben nicht oder nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können. Bestünde stets eine Pflicht, sich mit seinem Klarnamen bei einem Telemediendienst anzumelden, wäre eine Zuordnung für den Diensteanbieter indes immer ohne größeren Aufwand möglich. Zudem weist die in

---

[1158] https://www.datenschutz-hamburg.de/news/detail/article/der-hamburgische-datenschutzbeauftragte-profilnamen-bei-facebook-frei-waehlbar.html?tx_ttnews[backPid]=1&cHash=c2a6cea29f0fd07dae7ca92f86c724cc; auch das VG Hamburg hat indes im Verfahren des einstweiligen Rechtsschutzes deutschen Datenschutzrecht für unanwendbar erklärt und entsprechend die aufschiebende Wirkung des von Facebook gegen den Bescheid eingelegten Widerspruchs wiederhergestellt, VG Hamburg, ZD 2016, 243 (244 ff.); ausführlich zu dem Beschluss bereits oben unter C.II.4.b)cc). Das OVG Hamburg hat mit Beschluss vom 29.6.2016, ZD 2016, 450 (451 ff.) die vom Hamburger Datenschutzbeauftragten hiergegen eingelegte Beschwerde zurückgewiesen. Das OVG hat sich dabei allerdings nicht den rechtlichen Ausführungen des VG Hamburg angeschlossen, sondern unter Verweis auf das vom BVerwG angestrengte Vorabentscheidungsverfahren v. 25.2.2016, Rs. 1 C 28/14 (ZD 2016, 393 (393 ff.)) vor dem EuGH den Ausgang des Hauptsacheverfahrens für offen erklärt und nur in der vorläufigen Interessenabwägung die Interessen Facebooks an der aufschiebenden Wirkung als höher gewichtet.

[1159] *Moos*, in: Taeger/Gabel, § 13 TMG, Rn. 49; *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 22.

[1160] *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 22.

[1161] *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 22; *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 89; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 149 f.; vgl. auch *Hullen/Roggenkamp*, in: Plath, § 13 TMG, Rn. 43.

[1162] So auch bereits *Nietsch*, Anonymität, S. 107 ff.; vgl. auch *Schnabel/Freund*, CR 2010, 718 (719 f.); *Lauber-Rönsberg*, MMR 2014, 10 (12 f.).

§ 13 Abs. 6 TMG normierte Pflicht, eine Bezahlung pseudonym oder anonym zu ermöglichen, darauf hin, dass der Gesetzgeber auch das Verhältnis zwischen dem Nutzer und dem Anbieter von der Vorschrift erfasst sehen wollte.[1163] Ginge es nur um die pseudonyme Nutzung eines Dienstes nach außen, hätte sich eine Regelung dieses ausschließlich zwischen Anbieter und Nutzer stattfindenden Prozesses erübrigt. Dass hierdurch Erschwernisse bei der Rechtsverfolgung und -durchsetzung auftreten können, wurde vom Gesetzgeber gesehen und ausweislich der Gesetzesbegründung zu der Vorgängervorschrift des § 4 TDDSG ausdrücklich in Kauf genommen.[1164] Das Recht auf anonyme Nutzung besteht daher im Grundsatz auch gegenüber dem Anbieter eines Telemediendienstes.[1165]

Eine anonyme Registrierung ist allerdings speziell für die Anbieter sozialer Netzwerke in aller Regel unzumutbar i.S.v. § 13 Abs. 6 S. 1 letzter Hs.[1166] Sie würde tatsächlich zu einer Pflicht führen, anonyme Verträge abzuschließen und damit einen erheblichen Eingriff in die Vertragsfreiheit begründen. Anders als beispielsweise bei der Nutzung von Internetforen ist die Erstellung eines Profils in einem sozialen Netzwerk häufig auf Langfristigkeit ausgelegt. Zudem kann das Angebot des sozialen Netzwerks Funktionen eines Bezahldienstes und Möglichkeiten für sonstige finanzielle Transaktionen beinhalten, insbesondere wenn im Rahmen des sozialen Netzwerks auf kostenpflichtige Angebote Dritter zurückgegriffen wird. Das Interesse der Anbieter sozialer Netzwerke daran, ihre Vertragspartner identifizieren zu können, ist hier im Regelfall höher zu gewichten als das Interesse an der Möglichkeit einer anonymen Nutzung ihrer Dienste.[1167]

Die Unzumutbarkeit ergibt sich darüber hinaus aus der telemedienrechtlichen Zurechnung der Inhalte der Nutzer.[1168] Anbieter sozialer Netzwerke haften als Hostprovider für rechtsverletzende Inhalte gemäß den allgemeinen Vorschriften, ggf. modifiziert durch die §§ 8-10 TMG sowie § 7 Abs. 2 TMG. Diese sehen freilich erhebliche Privilegierungen vor, aufgrund

---

1163 So auch *Nietsch*, Anonymität, S. 108.

1164 Vgl. BT-Drs. 13/7385, S. 71.

1165 *Nietsch*, Anonymität, S. 107 ff.; *Caspar*, ZRP 2015, 233 (234); *Lauber-Rönsberg*, MMR 2014, 10 (12 f.); *Kremer*, CR 2012, 438 (442); *Feldmann*, K&R 2012, 113 (115); *Schnabel/Freund*, CR 2010, 718 (719 f.); vgl. allgemein zur Bedeutung der grundsätzlichen Möglichkeit einer anonymen Internetnutzung *Heckmann*, NJW 2012, 2631 (2632 f.).

1166 Vgl. *Maisch*, Informationelle Selbstbestimmung, S. 190 f.; *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 22; *Hullen/Roggenkamp*, in: Plath, § 13 TMG, Rn. 43; *Moos*, in: Taeger/Gabel, § 13 TMG, Rn. 49; *Stadler*, ZD 2011, 57 (58); *Schnabel/Freund*, CR 2010, 718 (720); a.A. *Kremer*, CR 2012, 438 (442); *Feldmann*, K&R 2012, 113 (115).

1167 Vgl. allgemein bereits *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG Rn. 22: *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 149.

1168 So auch *Hullen/Roggenkamp*, in: Plath, § 13 TMG, Rn. 43.

derer eine Zumutbarkeit der anonymen Nutzung teilweise dennoch bejaht wird.[1169] Insbesondere können Host-Provider gemäß § 10 Nr. 2 TMG nicht für fremde Informationen von Nutzern verantwortlich gemacht werden, sofern sie eine rechtswidrige Information unverzüglich löschen oder sperren, sobald sie von dieser Kenntnis erlangt haben. Ähnliche Privilegierungen werden im Rahmen der zivilrechtlichen Störerhaftung durch die Statuierung zumutbarer Prüfpflichten realisiert.[1170] Nach Ansicht mancher Autoren ist es für die Anbieter sozialer Netzwerke daher nicht zwingend erforderlich, den Urheber der Rechtsverletzung identifizieren zu können.[1171] Dieser Auffassung ist zugute zu halten, dass insbesondere im Falle von Urheberrechtsverletzungen private Auskunftsansprüche gemäß § 101 Abs. 9 UrhG direkt gegen den Internet-Provider bestehen[1172], wodurch die IP-Adresse und damit auch die Identität eines Rechtsverletzers ermittelt werden können auch wenn der Anbieter des sozialen Netzwerks den Klarnamen des Nutzers nicht kennt.

Es würde für die Anbieter sozialer Netzwerke aber einen unzumutbaren Aufwand bedeuten, wenn sie ausschließlich repressiv auf begangene Rechtsverletzungen reagieren könnten. Dies wäre aber die Konsequenz, wenn die bloße Erstellung eines anonymen Profils noch keinen Sperrgrund darstellen würde. Angesichts der Schwere denkbarer Verletzungen des Persönlichkeitsrechts in sozialen Netzwerken ist diese Perpetuierung von Rechtsverletzungen als Voraussetzung für eine Löschung nicht wünschenswert.[1173] Natürlich bliebe auch hier die Möglichkeit für Nutzer, ein Profil unter falschem Namen zu erstellen und sogar die eigene IP-Adresse zu verschleiern, beispielsweise durch Proxy-Server oder Virtual Private Networks (VPN-Clients). Eine Pflicht, sich mit Klarnamen zu registrieren, gibt den Anbietern sozialer Netzwerke aber zumindest das Recht, neu angelegte Profile von wiederholt die Nutzungsbedingungen verletzenden Personen präventiv zu sperren – sofern sie diese technisch erkennen können – und gegebenenfalls eine Klage auf Unterlassung anzustrengen.

Auch die im vorigen Abschnitt unter D.II.1 analysierte Regelung des § 55 Abs. 1 RStV spricht dafür, ein Recht auf eine anonyme Registrierung in sozialen Netzwerken abzulehnen. Das dort normierte Haushaltsprivileg beruht ausweislich der Gesetzesbegründung gerade auf der Überlegung, dass ein Verzicht auf ein Impressum bei privater Nutzung akzeptabel ist, weil

[1169] Vgl. *Kremer*, CR 2012, 438 (442); *Feldmann*, K&R 2012, 113 (115).
[1170] Zum Verhältnis der §§ 8-10 TMG und der zivilrechtlichen Störerhaftung bereits oben unter D.I.3.a)bb)i)
[1171] Ein Recht zur anonymen Registrierung deswegen bejahend: *Kremer*, CR 2012, 438 (442); *Feldmann*, K&R 2012, 113 (115).
[1172] Vgl. BGH, NJW 2012, 2958 (2958 f.), Rn. 9 f.; *Nietsch*, Anonymität, S. 94.
[1173] Vgl. auch *Krohm/Müller-Peltzer*, ZD 2015, 409 (412); *Peifer*, NJW 2014, 3067 (3069).

„über den Plattformanbieter sichergestellt [ist], dass die schutzwürdigen Belange der Beteiligten gewahrt werden können“[1174]. Dem Anbieter des sozialen Netzwerks wird somit die telemedienrechtliche Verantwortlichkeit für das Verhalten seiner Nutzer zugewiesen. In der klassischen Zwei-Personen-Konstellation eines Anbieters und eines Nutzers, die dem Datenschutz- und Telemedienrecht gedanklich immer noch zugrunde liegt, ist diese Aufteilung auch richtig: Der Diensteanbieter kontrolliert in dieser Konstellation das Angebot, profitiert von ihm und gestaltet es.

Das in sozialen Netzwerken vorliegende Mehrpersonenverhältnis sprengt diese Vorstellung. Auch Nutzern, die das Netzwerk ausschließlich zu persönlichen und familiären Zwecken im Sinne des § 55 Abs. 1 TMG nutzen, kommt eine Reichweite und Gestaltungshoheit zu, die herkömmlich Telemedienanbietern vorbehalten waren. Wie zuvor analysiert, ist es dennoch angezeigt, ihnen nach außen grundsätzlich eine pseudonyme Nutzung zu ermöglichen. Auch insoweit muss sich aber niederschlagen, dass diese Nutzer erheblich von der ursprünglichen Konzeption des Gesetzgebers eines ausschließlich nutzenden Nutzers abweichen: Durch ihre erhöhte Reichweite und Gestaltungshoheit vergrößern sie das Maß der dem Anbieter des sozialen Netzwerks zugerechneten Inhalte erheblich. Nimmt man den Ansatz der §§ 5 Abs. 1 TMG und 55 RStV ernst, einen namentlich Verantwortlichen für die Inhalte von Telemedien zu haben und dies über die Verbindung aller Nutzer zu dem Plattformbetreiber sicherzustellen, ist es nur folgerichtig, im Innenverhältnis von Anbietern und Nutzern sozialer Netzwerke ein Recht auf anonyme Registrierung abzulehnen.[1175]

Das Recht auf anonyme Nutzung gemäß § 13 Abs. 6 TMG besteht somit grundsätzlich auch gegenüber Diensteanbietern wie den Anbietern sozialer Netzwerke. Es ist diesen aber unzumutbar, eine anonyme Registrierung zwingend zu ermöglichen, sofern ihre Nutzer mit ihren Profilen eine Reichweite und inhaltliche Gestaltungsfreiheit erlangen, die sie vergleichbar zu klassischen Telemedienanbietern machen. Anders als etwa in vielen Diskussionsforen, in denen Nutzer einzelne Beiträge posten können, aber keinen Einfluss auf die Gesamtgestaltung haben, ist dies bei Profilen in sozialen Netzwerken in aller Regel der Fall. Nutzer in sozialen Netzwerken können sich daher regelmäßig nicht auf § 13 Abs. 6 TMG berufen, um eine anonyme Registrierung zu verlangen. Ein in den Nutzungsbedingungen statuierter

[1174] LT-BW-Drs. 14/558, S. 39.

[1175] Freilich steht es Anbietern sozialer Netzwerke dennoch frei, darauf zu verzichten, eine Registrierung unter dem Klarnamen zu verlangen, wenn sie diese Zurechnung in Kauf nehmen wollen, ohne die Verantwortung weitergeben zu können. Anonyme soziale Netzwerke wie etwa das Projekt www.ello.co sind daher zulässig.

Klarnamenzwang bei der Registrierung ist foglich zulässig, sofern die Daten ausschließlich dem Anbieter des sozialen Netzwerks zugänglich sind und nicht öffentlich gemacht werden.

III. Informations- und Machtgefälle

Ein Bedürfnis für staatliche Regulierung sozialer Netzwerke folgt auch aus den strukturellen Informations- und Machtgefällen in diesen.[1176] Die Anbieter sozialer Netzwerke haben einen substantiellen Informationsvorsprung gegenüber ihren Nutzern, ebenso wie gegenüber dem Staat, in der Frage, mit welchen Mitteln zu welchen Zwecken sie Daten erheben und verarbeiten. Außenstehende haben zunächst keine Möglichkeiten, die Datenverarbeitung zu kontrollieren oder bestimmte Verhaltensweisen zu unterbinden, da es sowohl an einer entsprechenden Verhandlungsmacht als auch an einem Einblick in die inneren Abläufe mangelt. Die Anbieter sozialer Netzwerke können dem individuellen Nutzer ihre Vertragsbedingungen daher weitgehend unbeeinflusst vorgeben. Insoweit ist es zwar sehr zu begrüßen, dass sich zunehmend Verbraucherschutzverbände berufen fühlen, gegen benachteiligende Klauseln insbesondere in Facebooks AGB oder Datenrichtlinien vorzugehen.[1177] Sie verändern aber noch nicht das grundsätzlich bestehende Macht- und Informationsgefälle zulasten der Nutzer und des Staates.

Für die individuelle Nutzung von sozialen Netzwerken erlangt dieses Gefälle vor allem mit Blick auf die Möglichkeit und Wirksamkeit von datenschutzrechtlichen Einwilligungen Bedeutung. Im Folgenden führt ein kursorischer Überblick in die Probleme der Einwilligung im Internet im Allgemeinen ein, welche sodann auf die strukturellen Probleme in sozialen Netzwerken konkretisiert werden. Im Kern geht es um die übergeordnete Frage, ob die Einwilligung tatsächlich ein geeignetes regulatorisches Mittel darstellt, um die individuelle Selbstbestimmung der Nutzer sicherzustellen (dazu 1. und 2.).

Soweit sich bei der Einwilligung Defizite auftun, werden darüber hinaus alternative Konzepte zur Absicherung der informationellen Selbstbestimmung besprochen, insbesondere die Ansätze des Selbstdatenschutzes und des sogenannten „Risk-Based Approach“ (dazu 3.). Anschließend folgt ein kurzer Ausblick auf die generelle Legitimität und mögliche Effektivität von

---

[1176] Vgl. *Piltz*, Soziale Netzwerke, S. 2; *Klar*, DÖV 2013, 103 (107); *Gurlit*, NJW 2010, 1035 (1039 f.); *Fehling*, Evolving Law and Economics of Internet Privacy, in: Eger u.a. (Hrsg.), Economic Analysis of International Law, S. 105 f.; *Hoffmann-Riem*, AöR 2012, 509 (533 ff.); allgemein zum Machtgefälle in Konstellationen moderner Datenanalyse *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 29 ff., 34 f.; *Mayer-Schönberger*, Die Tugend des Vergessens, S. 118 ff., 129 ff.; *Bäcker*, Der Staat (51) 2012, 91 (105 f.); *Greve*, Drittwirkung, in: FS Kloepfer, S. 670 f.

[1177] Vgl. z.B. KG Berlin, ZD 2014, 412 (412 ff.); LG Berlin, ZD 2015, 133 (133 ff.); zur Rolle von Verbandsklagerechten im Datenschutz noch unten unter D.III.3.a)cc).

paternalistischen Regelungen im Zusammenhang mit sozialen Netzwerken, wobei der Schwerpunkt auf Maßnahmen des sogenannten libertären Paternalismus liegt (dazu 4.).

1. Überblick: Die datenschutzrechtliche Einwilligung im Internet als dogmatischer Problemfall

Die Einwilligung im Internet im Allgemeinen, aber auch in sozialen Netzwerken im Besonderen ist in letzter Zeit vermehrt Gegenstand wissenschaftlicher Untersuchungen gewesen.[1178] Angesichts der zahlreichen Probleme, die sich im Zusammenhang mit diesem Rechtsinstitut ergeben, ist dies nicht verwunderlich. So erlangt sie insbesondere im Internet in sehr unterschiedlichen Rechtsbereichen wie dem Urheberrecht, dem Persönlichkeitsrecht und dem Datenschutzrecht mit jeweils unterschiedlichen Voraussetzungen Relevanz.[1179] Streit besteht indes schon über sehr grundlegende Fragen wie etwa die nach ihrer Rechtsnatur.[1180] Speziell im Datenschutzrecht ist umstritten, in welchem Verhältnis die Einwilligung zu den gesetzlichen Erlaubnistatbeständen oder gar Verpflichtungen zur Datenverarbeitung steht; ob es sich nur um eine optionale Ergänzung handelt oder um einen gleichwertigen, exklusiven Erlaubnistatbestand – mit Konsequenzen für die Folgen eines Widerrufs der Einwilligung.[1181] Ebenso bestehen teilweise Unklarheiten darüber, in welchem Verhältnis die Einwilligungsvorschriften in § 4a BDSG und § 13 Abs. 2 TMG zueinander stehen.[1182] Weiterhin wird im Datenschutzrecht lebhaft diskutiert, unter welchen Voraussetzungen eine Einwilligung im Internet wirksam eingeholt werden kann, und ob hierfür tatsächlich das vom BGH gebilligte Opt-Out-Prinzip genügt[1183] oder ob nicht doch stets ein Opt-In erforderlich ist.[1184] Zuletzt besteht Unklarheit darüber, unter welchen Voraussetzungen tatsächlich von einer informierten und freiwilligen Einwilligung ausgegangen werden kann und wie detailliert die

---

[1178] Vgl. jeweils m. zahlreichen w.N.: *Radlanski*, Das Konzept der Einwilligung; *Zimmermann*, Die Einwilligung im Internet; *Rogosch*, Die Einwilligung im Datenschutzrecht; *Buchner*, Informationelle Selbstbestimmung, S. 231 ff.; vgl. auch *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 31 ff.

[1179] *Zimmermann*, Einwilligung im Internet, S. 1 f.; vgl. den Überblick bei *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 47 ff., 76 ff.

[1180] *Zimmermann*, Einwilligung im Internet, S. 3 ff.; *Radlanski*, Das Konzept der Einwilligung, S. 117 ff.; *Simitis*, in: Simitis, BDSG, § 4 Rn. 20; *Rogosch*, Einwilligung im Datenschutzrecht; S. 36 ff.; *Buchner*, Informationelle Selbstbestimmung, S. 236 ff.; *Taeger*, in: Taeger/Gabel, § 4a BDSG, Rn. 29; *Kühling*, in: Wolff/Brink, § 4a BDSG, Rn. 32.

[1181] *Simitis*, in: Simitis, BDSG, § 4 Rn. 6 f.; *Taeger*, in: Taeger/Gabel, § 4a BDSG, Rn. 83; *Schneider/Härting*, ZD 2011, 63 (65).

[1182] Ausführlich: *Zimmermann*, Einwilligung im Internet, S. 40 ff.

[1183] Vgl. BGH, NJW 2008, 3055 (3056) – Payback; BGH, MMR 2010, 138 (139 f.) – Happy Digits.

[1184] Für ein Opt-In plädieren beispielsweise *Rogosch*¸ Einwilligung im Datenschutzrecht, S. 120 ff.; *Spindler/*Nink, in: Spindler/Schuster, § 13 TMG, Rn. 13; *Moos*, in: Taeger/Gabel, § 13 TMG Rn. 21; jedenfalls kritisch gegenüber Opt-Out Regelungen: *Däubler*, in: DKWW, § 4a BDSG Rn. 23a; *Schreibauer*, in: Auernhammer, § 13 TMG Rn. 37.

dem Betroffenen zur Verfügung gestellten Informationen sein müssen, ohne den Effekt der Aufklärung durch ein Übermaß an Informationen oder aber zu pauschale Aussagen zu konterkarieren.[1185]

Es würde den Rahmen dieser Arbeit sprengen, eine Antwort auf jede dieser teilweise sehr komplexen Fragen zu suchen. Der Untersuchungsansatz ist daher strikt auf die Bedeutung und Leistungsfähigkeit der Einwilligung in sozialen Netzwerken begrenzt. Um Erkenntnisse zu gewinnen, die langlebiger sind als die nächste Überarbeitung der Datenrichtlinien der Anbieter sozialer Netzwerke, insbesondere von Facebook, soll das Augenmerk besonders auf strukturelle Aspekte gelegt werden, weniger auf die aktuell gültigen, regelmäßigen Änderungen unterliegenden konkreten Datenrichtlinien. Im Kern geht es somit um die Frage, inwieweit die Einwilligung der Nutzer ihrer Funktion nachkommen kann, ein „manifestes Zeichen ihrer verfassungsrechtlich garantierten informationellen Selbstbestimmung“[1186] zu sein oder ob sie sich tatsächlich als bloße Fiktion erweist.[1187]

2. Leistungsfähigkeit der Einwilligung in sozialen Netzwerken

Die Verarbeitung von Nutzerdaten ist das zentrale Geschäftsmodell sozialer Netzwerke. Von ihm profitieren die Anbieter sozialer Netzwerke, aber auch Dritte als Werbepartner, die Betreiber von Fanpages, Verwender von Social PlugIns und Entwickler von „sonstigen Inhalten“ wie Spielen und anderen Apps. Wie bereits oben unter D.I.3 analysiert, sind diese Akteure, wenngleich in unterschiedlichem Maße, datenschutzrechtlich verantwortliche Stellen. Wie ebenfalls gezeigt wurde, sind wesentliche Teile der erfolgenden Datenverarbeitung nicht durch die gesetzlichen Erlaubnisnormen der §§ 28, 29 BDSG, §§ 11 ff. TMG bzw. zukünftig Art. 6 Abs. 1 lit. b-f) DS-GVO gedeckt und bedürfen daher gemäß § 4 Abs. 1 BDSG bzw. § 12 Abs. 1 TMG und zukünftig Art. 6 Abs. 1 lit. a) i.V.m. Art. 7 DS-GVO einer wirksamen Einwilligung der Betroffenen, um zulässig zu sein.

[1185] *Däubler*, in: DKWW, § 4a BDSG Rn. 18 f., 33; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 77 f.; *Radlanski*, Das Konzept der Einwilligung, S. 210 ff.; *Buchner*, Informationelle Selbstbestimmung, S. 103 ff.; allgemein zu möglichen schlechteren Entscheidungen aufgrund eines Mehrs an Informationen *Eidenmüller*, JZ 2011, 814 (816) m.w.N.

[1186] *Simitis*, in: Simitis, BDSG, § 4 Rn. 2 m.w.N.; vgl. auch *Däubler*, in: DKWW, § 4a BDSG, Rn. 2a; *Bäcker*, in: Wolff/Brink, Datenschutzrecht, § 4a BDSG, Rn. 1 m.w.N.; *Masing*, NJW 2012, 2305 (2307).

[1187] So *Simitis*, in: Simitis, BDSG, § 4 Rn. 3 m.w.N.; *Däubler*, in: DKWW, § 4a BDSG, Rn. 2a; *Bäcker*, in: Wolff/Brink, Datenschutzrecht, § 4a BDSG, Rn. 3; *Schneider/Härting*, ZD 2011, 63 (66); vgl. auch *Piltz*, Soziale Netzwerke, S. 119; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 91.

a) Einschlägige Rechts- und Formvorschriften für die Einwilligung

aa) Die Einwilligung nach der DS-GVO

Auch zukünftig können Betroffene in eine Datenverarbeitung gemäß Art. 6 Abs. 1 lit. a) i.V.m. Art. 7 DS-GVO einwilligen. Wie bisher auch muss sie frei, informiert und hinreichend bestimmt erfolgen, wie Art. 7 Abs. 4 i.V.m. Erwägungsgrund 32 DS-GVO klarstellt. Anders als nach bisherigem deutschen Recht[1188] sind nunmehr auch konkludente Einwilligungen möglich, welche nach Erwägungsgrund 32 DS-GVO allerdings durch eine eindeutig bestätigende Handlung und unmissverständlich bekundet werden muss.[1189] Eine Einwilligung bedarf somit – anders als gegenwärtig noch nach § 4a i.V.m. § 126a BGB – keiner eigenhändigen Unterschrift mehr; insbesondere reicht es in Zukunft aus, ein Häkchen hinter einer Einwilligungserklärung zu setzen. Dies ist durchaus zu begrüßen, da – wie sogleich unter bb) besprochen – das Erfordernis der eigenhändigen Unterschrift im digitalen Kontext nicht mehr zeitgemäß ist.[1190] Das Abgrenzungsproblem der Einwilligungserklärung nach § 13 Abs. 2 TMG und einer nach § 4a i.V.m. § 126a BGB wird sich damit unter Geltung der DS-GVO erübrigen. Der erwähnte Streit um ein Opt-In oder Opt-Out wird zugunsten eines strikten Opt-In Prinzips entschieden.

Art. 7 Abs. 3 DS-GVO normiert, dass die Einwilligung, wie bisher auch, zu jedem Zeitpunkt widerrufen werden kann und dass dies ohne Schwierigkeiten möglich sein muss. Er stellt zudem klar, dass der Widerruf nur *ex nunc* gilt und damit die Rechtmäßigkeit der Datenverarbeitung zeitlich vor dem Widerruf nicht berührt. Der Einwilligende ist über dieses Widerrufsrecht zu informieren.

Zum besonderen Schutz der Selbstbestimmung des Einwilligenden hatte der Kommissionsentwurf ursprünglich in Art. 7 Abs. 4 DS-GVO-E a.F. vorgesehen, dass eine Einwilligung nicht möglich sein sollte, sofern ein erhebliches Machtgefälle zwischen dem Datenverarbeiter und dem Betroffenen vorliegt. Diese Klausel wurde in den folgenden Entwürfen gestrichen und durch das aus der bisherigen Rechtslage bekannte Kopplungsverbot ersetzt.[1191] Erwägungsgrund 43 DS-GVO greift das frühere Verbot der Einwilligung im Falle

---

[1188] Zur bisherigen Rechtslage *Simitis*, in: Simitis, BDSG, § 4a Rn. 43 f. m.w.N.; vgl. auch *Kühling/Martini*, EuZW 2016, 448 (451).

[1189] *Dammann*, ZD 2016, 307 (307).

[1190] So auch *Keppeler*, MMR 2015, 779 (782); vgl. auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 79, 109.

[1191] Zum Kopplungsverbot unten unter D.III.2.b)cc); vgl. auch *Roßnagel/Kroschwald*, ZD 2014, 495 (497); *Kühling/Martini*, EuZW 2016, 448 (451).

eines erheblichen Machtgefälles allerdings abgeschwächt als Indiz dafür auf, dass die Einwilligung nicht freiwillig im Sinne der Vorschriften erfolgt ist.

Neu ist eine ausdrückliche Regelung der Einwilligung durch Minderjährige: Gemäß Art. 8 Abs. 1 DS-GVO soll eine Einwilligung für unter 16-Jährige nur mit Zustimmung ihrer gesetzlichen Vertreter möglich sein, wobei diese Altersgrenze durch mitgliedstaatliche Regelungen bis zu einem Alter von 13 Jahren herabgesenkt werden kann.[1192] Die Altersgrenze entspricht weitgehend der bisherigen Praxis der Nutzungsbedingungen sozialer Netzwerke, so dass sich insofern keine großen praktischen Änderungen ergeben.[1193] Man kann freilich daran zweifeln, ob 13 Jahre bereits ein angemessenes Alter für derartige Einwilligungen ist;[1194] dennoch ist die gesetzliche Klarstellung grundsätzlich zu begrüßen.

Die DS-GVO setzt somit keine entscheidenden neuen Impulse, was die Einwilligung betrifft. Kleinere Abgrenzungsprobleme werden gelöst, aber die großen Fragen, insbesondere die nach der hinreichenden Bestimmtheit der Einwilligung ebenso wie die nach der Freiwilligkeit der Einwilligung bleiben unbeantwortet. Die aktuelle Diskussion zu diesen Problemen wird sich daher nahtlos fortsetzen und die Erkenntnisse aus der bisherigen Rechtslage werden sich insofern übertragen lassen.

bb) Die Einwilligung nach bisheriger Rechtslage

In der bisherigen Rechtslage existieren zahlreiche, nicht abschließend geklärte Abgrenzungsprobleme, inwiefern eine Einwilligung nach dem TMG, dem TKG oder dem BDSG zu erfolgen hat. Welche Vorschriften einschlägig sind, ist vor allem abhängig von der Art der verarbeiteten Daten.[1195] Insbesondere die Frage, was ein erforderliches Nutzungsdatum im Sinne von § 15 TMG in Abgrenzung zu einem – gesetzlich nicht definierten – Inhaltsdatum darstellt, kann indes problematisch sein. So stellen Hobbies und Wohnort eines Nutzers nicht grundsätzlich Daten dar, die erforderlich sind, um den Dienst des sozialen Netzwerks technisch zu erbringen. Allerdings könnte man argumentieren, dass es auch gerade der Zweck sozialer Netzwerke ist, dass Nutzer sich gegenseitig finden und identifizieren können. Entsprechend wird vertreten, diese Daten nicht als Inhaltsdaten, sondern als Nutzungsdaten nach § 15 TMG

[1192] Vgl. ausführlich *Gola/Schulz*, ZD 2013, 475 (476 ff.).
[1193] Hierzu noch ausführlicher unten unter D.III.4.c)bb); vgl. auch *Gola/Schulz*, ZD 2013, 475 (480); *Kipker/Voskamp*, DuD 2012, 737 (740).
[1194] Vgl. *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 336; *Dies./Ders.*, MMR 2011, 637 (638); sehr kritisch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 107.
[1195] Zur Unterscheidung von Verkehrs-, Bestands-, Nutzungs- und Inhaltsdaten bereits ausführlich oben unter C.III.

einzuordnen.[1196] Allein auf die Art der Daten abzustellen, würde somit eine erhebliche Rechtsunsicherheit begründen.[1197] Entsprechend vielfältig ist das Meinungsspektrum darüber, wie eine zielgerichtetere Abgrenzung vorgenommen werden kann, ohne dass sich hierbei bereits eine klar erkennbare herrschende Meinung herauskristallisiert hätte.[1198] In sozialen Netzwerken ist die Abgrenzung vor allem für die Feststellung relevant, ob eine Einwilligung unter Einhaltung der einfachen elektronischen Form des § 13 Abs. 2 TMG erfolgen kann oder ob eine qualifizierte elektronische Einwilligung gemäß § 4a BDSG i.V.m. § 126a BGB mit einer entsprechenden Signatur erforderlich ist.[1199]

Soweit ein Datum sowohl als Bestands- oder Nutzungsdatum als auch als personenbezogenes Inhaltsdatum einzuordnen ist, wird verbreitet vertreten, standardmäßig das Erfordernis der Schriftform abzulehnen, weil besondere Umständen i.S.d. § 4a Abs. 1 S. 3 BDSG vorliegen sollen.[1200] Teilweise wird diese Ablehnung des Schriftformerfordernisses sogar generell auf die Erhebung und Verwendung von Inhaltsdaten über elektronische Medien ausgeweitet.[1201] Eine derartig weite Auslegung übergeht indes den ausdrücklichen Ausnahmecharakter der besonderen Umstände, der eine restriktive Auslegung gebietet.[1202] Die Erhebung und Verarbeitung von Inhaltsdaten durch Anbieter sozialer Netzwerke stellt einen alltäglichen und mitnichten besonderen Vorgang dar. Es überzeugt nicht, dass eine Anwendung des § 4a Abs. 1 S. 3 BDSG zu einem „Leerlaufen" des § 13 Abs. 2 TMG führen würde[1203], da dieser für die Verarbeitung von reinen Bestands- und Nutzungsdaten anwendbar bleibt. Aus systematischen Gründen und wortlautnaher Auslegung spricht daher viel dafür, eine kumulative Anwendbarkeit von § 4a BDSG und § 13 Abs. 2 TMG zu bejahen, was im Ergebnis die Geltung

---

1196 *Spindler/Nink*, in: Spindler/Schuster, § 15 Rn. 7; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 87; ausführlich zu den unterschiedlichen Zwecken sozialer Netzwerke und ablehnend zur Einordnung von Inhaltsdaten als Nutzungsdaten: *Karg/Fahl*, K&R 2011, 453 (453 f., 458); nach hier vertretener Ansicht handelt es sich bei nutzergenerierten Inhalten ausschließlich um Inhaltsdaten, um eine undifferenzierte Aufweichung des Begriffs der Nutzungsdaten mit erheblichen Abgrenzungsproblemen zu vermeiden, hierzu bereits oben unter C.III.4.b).

1197 *Zimmermann*, Einwilligung im Internet, S. 43; *Karg/Fahl*, K&R 2011, 453 (458).

1198 Ausführlicher Überblick bei *Zimmermann*, Einwilligung im Internet, S.45 ff., m. zahlreichen w.N.

1199 Zur Abgrenzung ausführlich *Rogosch*, Einwilligung im Datenschutzrecht, S. 159 ff.; vgl. auch bereits *Piltz*, Soziale Netzwerke, S. 122 ff.

1200 *Kramer* in: Auernhammer, § 4a BDSG Rn. 36; *Moos*, in: Taeger/Gabel, § 13 TMG Rn. 18; *Piltz*, Soziale Netzwerke, S. 124 f.; *Schreibauer*, in: Auernhammer, § 13 TMG Rn. 29.

1201 *Taeger*, in: Taeger/Gabel, § 4a BDSG, Rn. 35, 38 f.; *Raabe/Lorenz*, DuD 2011, 279 (284); offen gelassen von *Kühling*, in: Wolff/Brink, Datenschutzrecht, § 4a BDSG, Rn. 48, der lediglich konstatiert: Die „Anforderungen im Falle einer üblichen Anbahnung [dürfen] nicht überzogen werden, insbes. wenn der Vertrag per E-Mail oder mittels Eingabeformularen im „Internet" abgewickelt wird."; ein derart weites Verständnis ausdrücklich ablehnend: *Simitis*, in: Ders., BDSG, § 4a Rn. 38.

1202 *Simitis*, in: Ders., BDSG, § 4a Rn. 44; *Spindler/Nink*, in: Spindler/Schuster, § 4a BDSG, Rn. 11; *Däubler*, in: Ders. (u.a.), BDSG, § 4a Rn. 15; *Rogosch*, Datenschutz im Internet, S. 165 f.; *Holznagel/Sonntag*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 4.8 Rn. 29.

1203 So aber *Moos*, in: Taeger/Gabel, § 13 TMG Rn. 18.

der strengeren Formvorschrift bedeuten würde.[1204] Soweit es sich dagegen ausschließlich um personenbezogene Inhaltsdaten handelt, wäre ebenfalls die Schriftform des § 4a Abs. 1 S. 3 BDSG zu beachten.

Freilich würde das Erfordernis einer qualifizierten elektronischen Einwilligung gemäß § 126a BGB aktuell – soweit ersichtlich – von keinem sozialen Netzwerk erfüllt und wäre darüber hinaus auch sehr praxisuntauglich, da sich die Verwendung elektronischer Signaturen bisher nur wenig und vor allem im geschäftlichen Verkehr etabliert hat.[1205] Soziale Netzwerke sind auf Inhaltsdaten ihrer Nutzer angewiesen, um die Nutzung interessant zu machen und Werbeeinnahmen zu generieren. Soziale Netzwerke verlören somit einen bedeutenden Daseinszweck und ein Kernelement ihres Geschäftsmodells, würde die Erhebung dieser Inhaltsdaten durch ein derartig praxisfernes Formerfordernis faktisch unmöglich gemacht.

Einen Ausweg aus dem praktischen Dilemma bietet der im Rahmen der BDSG-Novelle von 2009 eingefügte § 28 Abs. 3a BDSG, welcher die einfache elektronische Form des § 13 Abs. 2 TMG in das allgemeine Datenschutzrecht übertragen hat, soweit es um die Verarbeitung von Inhaltsdaten für Zwecke des Adresshandels oder der Werbung gemäß § 28 Abs. 3 BDSG geht.[1206] Die Anbieter sozialer Netzwerke verarbeiten speziell auch Inhaltsdaten von Nutzern, um Werbeprofile zu erstellen. Entsprechend spricht viel dafür, die Erhebung und Verarbeitung dieser Daten unter das Formerfordernis des § 28 Abs. 3a BDSG zu subsumieren. Hiergegen lässt sich zwar einwenden, dass die Verarbeitung zu Werbezwecken einen von der Bereitstellung der Daten für andere Nutzer zu unterscheidenden Verarbeitungsschritt darstellt und die Bereitstellung jedenfalls auf den ersten Blick nicht dem Zweck der Werbung dient. Wie indes schon an mehreren Stellen festgestellt, ist es gerade Teil des Geschäftsmodells sozialer Netzwerke, alle ihnen zur Verfügung stehenden Daten zur Generierung weiterer Informationen und präziseren Persönlichkeitsprofilen zu Zwecken der Werbung zu nutzen.[1207] Auch die Übermittlung an und Bereitstellung der Daten für andere Nutzer dient daher jedenfalls mittelbar den in § 28 Abs. 3a BDSG genannten Zwecken der Werbung.

[1204] Ausführlich: *Rogosch*, Datenschutz im Internet, S. 162 ff.

[1205] *Taeger*, in: Taeger/Gabel, § 4a BDSG, Rn. 34; *Kühling*, in: Wolff/Brink, § 4a BDSG, Rn. 48; *Piltz*, Soziale Netzwerke, S. 124; *Raabe/Lorenz*, DuD 2011, 279 (280); vgl. auch *Rogosch*, Datenschutz im Internet, S.166 f.

[1206] Als Vorschlag *de lege ferenda* empfehlen eine generelle Integration der Regelung des § 28 Abs. 3a BDSG für Fälle der Internetkommunikation in § 4a BDSG *Raabe/Lorenz*, DuD 2011, 279 (284).

[1207] Hierzu bereits oben unter B.II.3.b).

Diese Auslegung mag aus Betroffenenperspektive rechtspolitisch ungünstig sein. Sie bietet allerdings deutlich mehr Rechtssicherheit und ist methodisch überzeugender, als die etwas konstruiert wirkende Lösung, zweifelsfreie Inhaltsdaten als Nutzungsdaten zu behandeln und damit zu einer Anwendbarkeit des § 13 Abs. 2 TMG zu gelangen[1208] oder den Wortlaut der besonderen Umstände in § 4a Abs. 1 S. 3 BDSG für so alltägliche Vorgänge zu überdehnen[1209].

Natürlich ist zu bedenken, dass das strengere Formerfordernis des § 4a BDSG in einer effektiveren Schutz- und Warnfunktion begründet ist.[1210] Eine Aufhebung dieses strengeren Schutzes gerade für soziale Netzwerke, die teilweise sogar sensible personenbezogene Daten im Sinne von § 3 Abs. 9 BDSG verarbeiten, bedeutet sicherlich eine Schlechterstellung der Betroffenen zugunsten eines einfacheren Datenumgangs. Dies ist indes eine zwingende Folge der Regelung des § 28 Abs. 6 i.V.m. § 4 Abs. 3 BDSG, wonach auch diese Daten für Zwecke der Werbung verarbeitet werden dürfen, solange sich der Betroffene hiermit nur ausdrücklich und auf diese Daten bezogen einverstanden erklärt.[1211] Ob eine solche Einwilligung hinreichend aufgeklärt und im Bewusstsein der möglichen Gefahren für die informationelle Selbstbestimmung möglich ist, ist aber keine Frage der Form, sondern Teil des größeren Problems, ob eine informierte, freiwillige Einwilligung gemäß § 4a Abs. 1 S. 1 BDSG in die Datenverarbeitung in sozialen Netzwerken überhaupt möglich ist, hierzu sogleich.

Zusammenfassend lässt sich damit festhalten, dass nach bisheriger nationaler Rechtslage für die Einwilligung in die Datenverarbeitung in sozialen Netzwerken je nach Art des Datums die Formvorschriften des § 13 Abs. 2 TMG oder des § 28 Abs. 3a BDSG beachtet werden müssen, welche sich indes praktisch nur unwesentlich voneinander unterscheiden.[1212]

Für Bestands- und Nutzungsdaten müssen darüber hinaus die materiellen Voraussetzungen des § 13 Abs. 1 und 2 TMG eingehalten werden, für Inhaltsdaten die materiellen Voraussetzungen des § 4a BDSG. Die Vorschriften überschneiden sich inhaltlich weitestgehend, insbesondere verlangen sie eine informierte, bewusste und freiwillige Entscheidung.[1213] Verbreitet wird auch vertreten, dass die allgemeinen Anforderungen von § 4 Abs. 3 BDSG i.V.m. § 4a BDSG,

---

[1208] So aber *Spindler/Nink*, in: Spindler/Schuster, § 15 TMG Rn. 7.

[1209] So aber *Piltz*, Soziale Netzwerke, S. 124 f.; *Moos*, in: Taeger/Gabel, § 13 TMG Rn. 18; *Taeger*, in: Taeger/Gabel, § 4a BDSG, Rn. 38 f.; *Kramer* in: Auernhammer, § 4a BDSG Rn. 36; *Raabe/Lorenz*, DuD 2011, 279 (284).

[1210] Statt vieler: *Simitis*, in: Simitis, BDSG, § 4a Rn. 33 ff.; *Kühling*, in: Wolff/Brink, § 4a BDSG Rn. 49.

[1211] Vgl. *Simitis*, in: Simitis, BDSG, § 28 Rn. 297 f.

[1212] Sollte sich darüber hinaus das Bedürfnis ergeben, Verkehrsdaten über die gesetzlichen Erlaubnistatbestände hinaus zu nutzen, so richtet sich die Wirksamkeit der Einwilligung nach § 94 TKG.

[1213] Vgl. *Spindler/Nink*, in: Spindler/Schuster, § 13TMG Rn. 3; *Taeger*, in: Taeger/Gabel, § 4a BDSG, Rn. 39.

abzüglich des Schriftformerfordernisses, stets ergänzend auf § 13 Abs. 2 TMG anzuwenden sind.[1214] Da die Anforderungen aber im Wesentlichen vergleichbar sind und die Abgrenzung nach den einzelnen Datenarten zur Bestimmung des Schriftformerfordernisses ab Anwendbarkeit der DS-GVO nicht mehr von Bedeutung sein wird, wird im Folgenden auf eine weitere präzise Abgrenzung verzichtet und stattdessen die übergeordnete Frage nach der hinreichenden Informiertheit und Freiwilligkeit untersucht.

b) Hinreichende Bestimmtheit, Informiertheit und Freiwilligkeit der Einwilligung

Damit eine Einwilligung nach Art. 7 DS-GVO und bisher § 4a Abs. 1 BDSG bzw. § 13 Abs. 1 und 2 TMG wirksam ist, muss sie auf der freien Entscheidung des Betroffenen beruhen und damit hinreichend bestimmt, informiert und freiwillig erfolgen.[1215] Die Freiwilligkeit wird hierbei über das in Art. 7 Abs. 4 i.V.m. Erwägungsgrund 43 DS-GVO normierte Kopplungsverbot abgesichert.

Der bisherige § 28 Abs. 3b BDSG stellt sich nach dem Wortlaut etwas strenger als Art. 7 Abs. 4 DS-GVO dar, da hiernach bereits der Abschluss eines Vertrags nicht von der Erteilung einer Einwilligung abhängig gemacht werden darf, wenn ein anderer Zugang zu gleichwertigen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist.[1216] Dies entspricht indes der Wertung des Erwägungsgrundes 42 DS-GVO, welcher zur Auslegung des Art. 7 Abs. 4 DS-GVO heranzuziehen ist, so dass davon auszugehen ist, dass sich insoweit keine Änderungen in der Rechtslage ergeben werden.

Sowohl in Bezug auf die Bestimmtheit und Informiertheit als auch die Freiwilligkeit der Einwilligung lassen sich gerade im Falle der Nutzung von Facebook erhebliche Zweifel anmelden. Wie in dieser Arbeit an verschiedenen Stellen gezeigt wurde, nutzt Facebook die anfallenden Daten seiner Nutzer zur Erstellung höchst detaillierter Persönlichkeitsprofile. Bei vielen dieser Daten dürfte den Nutzern nicht bewusst sein, dass sie anfallen und welche Aussagekraft sie in Kombination mit anderen Daten und im Rahmen einer Big Data Analyse entfalten können.[1217] Dies gilt insbesondere für die im Rahmen der Reichweitenanalyse durch

---

[1214] *Schreibauer*, in: Auernhammer, § 13 TMG Rn. 26; *Moos*, in: Taeger/Gabel, § 13 TMG Rn. 30; *Kremer*, CR 2012, 438 (442).

[1215] Statt vieler: *Simitis*, in: Simitis, BDSG, § 4a Rn. 62 f.; *Spindler/Nink*, in: Spindler/Schuster, § 13 TMG, Rn. 2 f., 8; Art. 29 DatSchGruppe, Stellungnahme 15/2011, WP 187, S. 7 ff.

[1216] Ausführlich: *Simitis*, in: Simitis, BDSG, § 4a Rn. 63 m.w.N.; *Taeger*, in: Taeger/Gabel, § 4a BDSG, Rn. 55 ff.

[1217] *Spiecker gen. Döhmann*, K&R 2012, 717 (720 f.); *Moser-Knierim*, ZD 2013, 263 (265); *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 71; vgl. auch *Spindler*, GRUR-Beilage 2014, 101 (103); *Mayer-Schönberger*, Die Tugend des Vergessens, S. 106 ff.; *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner, S. 431 f.

Social PlugIns gesammelten Daten im gesamten Internet, aber auch innerhalb des sozialen Netzwerks durch eine Analyse der dortigen Aktivitäten und „Likes".

aa) Datenrichtlinien im Spannungsfeld von Blankoeinwilligung und Überkomplexität

Facebook bemüht sich mittlerweile in seiner Datenrichtlinie um eine etwas ausführlichere Aufklärung, welche Daten es zu welchen Zwecken sammelt und an wen es diese weitergibt – in Folge einiger Gerichtsurteile, die diese als zu unbestimmt bewertet haben.[1218] In nur geringfügig polemischer Überspitzung lässt sich diese in ihrer aktuellen Version vom Januar 2015 dahingehend zusammenfassen, dass alle für Facebook irgendwie verfügbaren Daten gesammelt und verwendet werden. Dies gilt insbesondere für Daten, die im Zusammenhang mit der Nutzung von Facebook oder mit diesem verbundenen Diensten wie beispielsweise Social PlugIns oder ihm gehörenden Unternehmen anfallen. Verwendet werden diese Daten von Facebook, „um unsere Dienste anzubieten und zu unterstützen", welche pauschal aufgeschlüsselt werden in die Kategorien „Bereitstellung, Verbesserung und Entwicklung von Diensten", „Kommunikation mit dir", „Anzeigen und Messen von Werbeanzeigen und Diensten" und „Förderung der Sicherheit".[1219] Diese Unterkategorien bleiben indes sehr vage und mitnichten abschließend, so dass kein endgültiger Überblick darüber möglich ist, in welcher Form Daten konkret verwendet werden.[1220] Auch die Informationen über die

[1218] Vgl. KG Berlin, ZD 2014, 412 (418 ff.); LG Berlin, ZD 2015, 133 (134 ff.).

[1219] https://www.facebook.com/privacy/explanation (Stand 29. September 2016).

[1220] Unter der Kategorie „Bereitstellung, Verbesserung und Entwicklung von Diensten" findet sich beispielsweise die folgende Passage: „Wenn wir Standortinformationen haben, verwenden wir diese, um unsere Dienste für dich und andere individuell zu gestalten; z. B. indem wir dir beim Besuchen und Auffinden lokaler Veranstaltungen oder von Angeboten in deiner Umgebung helfen oder deinen Freunden mitteilen, dass du in der Nähe bist. Wir führen Umfragen und Studien durch, testen noch in der Entwicklung befindliche Funktionen und analysieren die Informationen, die wir haben, um Produkte und Dienstleistungen zu bewerten und zu verbessern, neue Produkte oder Funktionen zu entwickeln und Prüfungen sowie Aktivitäten zur Problem- oder Fehlerbehebung durchzuführen.", https://www.facebook.com/privacy/explanation (Stand 29. September 2016); vgl. auch *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 15, 67 ff.

Weitergabe der Daten an Dritte bleiben unbestimmt, da nicht abschließend aufgeführt ist, an wen Daten zu welchen Zwecken weitergegeben werden dürfen.[1221]

Es ist Facebook zuzugestehen, dass die Information, im Ergebnis alle verfügbaren Daten zu sammeln und diese in jeder erdenklichen Weise zu einer Maximierung des eigenen Umsatzes zu verwenden, insbesondere auch für neue, noch in der Entwicklung befindliche Funktionen, Produkte und Dienstleistungen, wohl eine akkurat zutreffende Beschreibung darstellt. Gleichzeitig muss man sich aber natürlich fragen, ob es sich bei einer solchen Erklärung nicht de facto bereits um eine Blanko-Einwilligung handelt, die aufgrund der fehlenden Überschaubarkeit und ihrer Unbestimmtheit völlig zurecht als unvereinbar mit § 4a Abs. 1 S. 1 BDSG und zukünftig entsprechend auch Art. 7 DS-GVO eingestuft wird.[1222] Darüber hinaus ist zumindest sehr fraglich, ob überhaupt von einer hinreichend bewusst und bestimmt erklärten Einwilligung ausgegangen werden kann, wenn Facebook seine Datenrichtlinien signifikant verändert und eine Einwilligung seiner Nutzer durch deren weitere Nutzung unterstellt, wie es immer wieder geschieht.[1223] Während dies zwar dem vom BGH gebilligten Opt-Out-Prinzip im Rahmen der elektronischen Einwilligungserteilung[1224] genügen mag, ist realistischerweise davon auszugehen, dass ein Großteil der Nutzer die veränderten Datenschutzbedingungen nicht oder nicht hinreichend zur Kenntnis genommen haben wird. Es kann auch schwerlich davon

---

[1221] In den Datenrichtlinien finden sich beispielsweise die folgenden Formulierungen: „Wenn du Apps, Webseiten oder sonstige Dienste Dritter verwendest, die unsere Dienste nutzen bzw. auf diesen integriert sind, erhalten sie möglicherweise Informationen darüber, was du postest oder teilst. […] Die von diesen Apps, Webseiten oder integrierten Dienstleistungen gesammelten Informationen unterliegen deren eigenen Bedingungen und Richtlinien."; „Wir teilen Informationen, die wir über dich haben, innerhalb der Gruppe von Unternehmen, die zu Facebook gehören. Mehr zu unseren Unternehmen."; „Sollten sich die Eigentums- oder Machtverhältnisse aller bzw. eines Teils unserer Dienste oder ihrer Vermögenswerte ändern, können wir deine Informationen an den neuen Eigentümer übertragen."; „Wir übertragen Informationen an Anbieter, Dienstleister und sonstige Partner, die unser Unternehmen weltweit unterstützen, beispielsweise indem sie Dienstleistungen für eine technische Infrastruktur zur Verfügung stellen, analysieren, wie unsere Dienste genutzt werden, die Wirksamkeit von Werbeanzeigen und Diensten messen, eine Kundenbetreuung anbieten, Zahlungen ermöglichen oder wissenschaftliche Studien und Umfragen durchführen. Diese Partner müssen im Einklang mit dieser Datenrichtlinie und den mit ihnen geschlossenen Vereinbarungen strenge Geheimhaltungspflichten einhalten.", https://www.facebook.com/privacy/explanation (Stand 29. September 2016); ebenfalls kritisch zur hinreichenden Bestimmtheit der Datenrichtlinien: *Buchner*, Facebook zwischen BDSG und UWG, in: FS Köhler, S. 52 ff.; *Martini/Fritzsche*, VerwArch (104) 2013, 449 (458 f.); *Maisch*, Informationelle Selbstbestimmung, S. 200.

[1222] Vgl. bereits *Buchner*, Facebook zwischen BDSG und UWG, in: FS Köhler, S. 54 f.; *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 68; *Martini/Fritzsche*, VerwArch (104) 2013, 449 (458 f.); *Kremer*, CR 2012, 438 (443); ausführlich zur Unvereinbarkeit von Blanko-Einwilligungen mit § 4a Abs. 1 S. 1 BDSG: statt vieler *Simitis*, in: Simitis, BDSG, § 4a Rn. 77 m. zahlreichen w.N.; *Kühling*, in: Wolff/Brink, § 4a BDSG, Rn. 44; *Buchner*, Informationelle Selbstbestimmung, S. 138 f.; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 50, 78; vgl. auch BVerfGK 9, 353 (360 f.) - Schweigepflichtentbindung; BGH, BGHZ 95, 362 (367 ff.); 116, 268 (273); *Ernst*, NJOZ 2010, 1917 (1919).

[1223] Vgl. *Martini/Fritzsche*, VerwArch (104) 2013, 449 (458).

[1224] Vgl. BGH, NJW 2008, 3055 (3056) – Payback; BGH, MMR 2010, 138 (139 f.) – Happy Digits; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 49.

ausgegangen werden, dass im Sinne von Erwägungsgrund 32 DS-GVO ein klares, informiertes und eindeutiges Einverständnis durch die Nutzer vorliegt. Die Einwilligung verkommt in diesem Verfahren damit zur bloßen Fiktion.

Diese Unsicherheiten weisen auf das grundsätzliche Problem mit der Informiertheit und Bestimmtheit der Einwilligung im Zusammenhang mit sozialen Netzwerken, aber auch zahlreichen anderen Formen moderner Datenverarbeitung hin: Eine abschließende Aufzählung aller Verwendungsphasen und -zwecke und ein umfassendes Update bei jeder Änderung würde zu einer überwältigenden Menge an Informationen führen, die keinesfalls Klarheit und Verständlichkeit erzeugen würde. Ein gewisses Maß an Unvollständigkeit ist daher stets hinzunehmen.[1225] Andererseits ist die Datensammlung insbesondere durch die Anbieter vieler sozialer Netzwerke und speziell Facebook derart umfassend, dass es jedenfalls unwahrscheinlich erscheint, dass Nutzer bei einer entsprechend verkürzten Information einen hinreichend konkreten Überblick erhalten. Vielmehr dürften auch derart verkürzte Informationen entweder viele Betroffene in ihrer Tragweite und ihrem Umfang überfordern oder aber zu unbestimmt bleiben.[1226] Entsprechend darf durchaus in Frage gestellt werden, ob eine informierte, hinreichend bestimmte Einwilligung in die umfassende Datenverarbeitung im Zusammenhang mit sozialen Netzwerken, insbesondere Facebook, überhaupt möglich ist.[1227] Die gegenwärtigen Datenrichtlinien erweisen sich in den analysierten Passagen jedenfalls als teilweise zu unbestimmt.

bb) Die verschobene Wahrnehmung von informatorischen Eingriffen

Ein weiteres Problem ist, dass die korrekte Einordnung von informatorischen Eingriffen sich grundsätzlich schwierig gestaltet: Die bloße Kenntnis eines Dritten von einer Information bedeutet noch keine unmittelbare Konsequenz für den Betroffenen. Diese Konsequenz erwächst vielmehr erst aus Handlungen, die der Dritte aufgrund der erhaltenen Information ergreift.[1228] Eben diese Handlungen Dritter können in Bezug auf die in sozialen Netzwerken erfolgende Datenauswertung sehr abstrakt und für den Einzelnen schlecht erkennbar sein. Wie oben im 1.

[1225] *Simitis*, in: Simitis, BDSG, § 4a Rn. 80; *Kühling*, in: Brink/Wolff, § 4a BDSG, Rn. 45; vgl. zum abnehmenden Grenznutzen zusätzlicher Informationen *Eidenmüller*, JZ 2011, 814 (816) m.w.N.; *Spindler*, GRUR-Beilage 2014, 101 (103); *ders.*, Gutachten F zum 69. dt. Juristentag, 2012, S. 78.

[1226] Vgl. *Masing*, NJW 2012, 2305 (2309); *Peifer*, K&R 2011, 543 (544 f.); *Martini/Fritzsche*, VerwArch (104) 2013, 449 (458); *Härting*, NJW 2013, 2065 (2070); *Spiecker gen. Döhmann*, K&R 2012, 717 (719); vgl. auch *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 31 f.

[1227] Vgl. *Kutscha*, GR-Schutz im Internet, S. 44 ff. m.w.N.; hierzu auch noch vertieft unten unter E.II.

[1228] *Spiecker gen. Döhmann*, K&R 2012, 717 (721); *Grimmelmann*, 94 Iowa L. Rev. 1137 (1160 f., 1066 ff.), 2008-2009; vgl. auch *Hermstrüwer*, Informationelle Selbstgefährdung, S. 284 ff.

Teil dargelegt wurde, handelt es sich hierbei mitnichten nur um etwas personalisierte Werbung. Vielmehr kann die Datenauswertung auch Auswirkungen auf beispielsweise eine Kreditvergabe oder die Kosten einer privaten Krankenversicherung haben, indem aus ihr erhöhte Risiken berechnet werden.[1229] Perfiderweise werden diese Ereignisse aber nicht unbedingt mit den Aktivitäten in sozialen Netzwerken in Verbindung gebracht werden – und eine konkrete Nachvollziehbarkeit ist für den Einzelnen ohnehin kaum gegeben. Verbunden mit dem Analysepotential, welches sich aus Big Data im Allgemeinen ergibt und eine Vorhersage individuellen Verhaltens basierend auf gruppentypischen Verhaltensmustern ermöglicht, erscheint es daher jedenfalls äußerst fragwürdig, von einer informierten, hinreichend bestimmten und freiwilligen Einwilligung in die Datenverarbeitung in sozialen Netzwerken auszugehen.[1230]

Dies gilt umso mehr, wenn man bedenkt, dass soziale Netzwerke durch ihre Aufmachung Entscheidungsprozesse manipulieren und zu einer Unterschätzung der mit ihnen verbundenen Risiken verleiten.[1231] Facebook, aber auch andere soziale Netzwerke, suggerieren eine abgeschlossene, private Sphäre, in welcher sich die Nutzer mit ihren Freunden austauschen können. Indem keine offensichtlichen Konsequenzen der Informationspreisgabe ersichtlich sind, wird eine objektive Einschätzung des mit der Nutzung verbundenen Risikos erheblich erschwert. Auch die intuitive Benutzeroberfläche und häufig spielerisch gestaltete Nutzerprofile erschweren eine kritsiche Reflektion über die mit der Nutzung verbundenen Risiken.[1232]

Gleichzeitig üben die zahlreichen anderen Nutzer insoweit eine trügerisch beruhigende Wirkung aus, da es für viele Menschen intuitiv plausibel sein dürfte, dass es innerhalb eines Schwarms sicher ist und sich sicherlich nicht *alle* anderen über die Sicherheit der Nutzung

[1229] Vgl. oben unter B.II.3.b)bb). Weitere Risiken analyisert *Maisch*, Informationelle Selbstbestimmung, S. 167 ff. und nennt dabei u.a. die Möglichkeit eines Daten- oder Identitätsdiebstahls sowie die Haftung für sog. „Facebook Partys".

[1230] So auch *Spiecker gen. Döhmann*, K&R 2012, 717 (720 f.); sehr ausführlich zur systematischen Fehleinschätzung von Datenschutzrisiken *Hermstrüwer*, Informationelle Selbstgefährdung, S. 271 ff. m.w.N.; vgl. auch allgemein *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 31 ff.; *Mayer-Schönberger*, Die Tugend des Vergessens, S. 121.; *Bäcker*, Der Staat (51) 2012, 91 (112 f.). Vgl. zur Übertragbarkeit des Konzepts des „mündigen Verbrauchers" unten unter E.II.1.

[1231] Ausführlich zum Folgenden: *Grimmelmann*, 94 Iowa L. Rev. 1137 (1160 ff.), 2008-2009; *Heckmann*, NJW 2012, 2631 (2633 f.); vgl. allgemein zur falschen Risikoeinschätzung, bzw. irrationalem Entscheidungsverhalten von Menschen aus verhaltensökonomischer Perspektive *Thaler/Sunstein*, Nudge, S. 31 ff.; *Eidenmüller*, JZ 2011, 814 (816 f.) m.w.N.

[1232] *Maisch*, Informationelle Selbstbestimmung, S. 167 f.

irren.[1233] Da aber nur die wenigsten Nutzer tatsächlich einen Überblick über die Risiken haben dürften, geht diese intuitive Annahme fehl und führt zu einer tendenziell schlecht informierten Entscheidung. Durch das ständige Wachstum speziell Facebooks handelt es sich hierbei um einen sich selbst verstärkenden Prozess.[1234]

cc) Gesellschaftliche Bedeutung sozialer Netzwerke und das Kopplungsverbot

Zuletzt bestehen erhebliche Zweifel an der Freiwilligkeit der Nutzung speziell Facebooks in jüngeren Altersgruppen. Wie im 1. Teil bereits gezeigt wurde, sind in der Gruppe der unter 29-Jährigen über 90% bei einem sozialen Netzwerk angemeldet, davon 83% bei Facebook.[1235] 89% von ihnen sind täglich in einem sozialen Netzwerk aktiv und nutzen dies unter anderem für Kommunikationszwecke, um Informationen über Veranstaltungen zu erhalten und um ihr Privatleben mit ihren Freunden zu organisieren.[1236] Es wäre lebensfremd, anzunehmen, dass dieser Verbreitungsgrad keinerlei sozialen Druck aufbaut, Mitglied in einem sozialen Netzwerk und speziell bei Facebook zu werden, um einen Ausschluss von der Kommunikation und der Planung von Verabredungen zu vermeiden.[1237] Tatsächlich ist daher sogar zu überlegen, ob die erzwungene Einwilligung in die Datenrichtlinien bei Facebook nicht sogar einen Verstoß gegen das Kopplungsverbot gemäß Art. 7 Abs. 4 DS-GVO bzw. § 28 Abs. 3b BDSG darstellt.[1238] Freilich muss dieses sehr eng verstanden werden und bezieht sich auf klar abgegrenzte Fallkonstellationen. Es richtet sich lediglich dagegen, einem Vertragspartner erzwungenen Zugang zu Informationen zu gewähren, die für die Erfüllung des Vertragszwecks nicht erforderlich sind.[1239]

1233 *Grimmelmann*, 94 Iowa L. Rev. 1137 (1161 f.), 2008-2009; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 280 ff.

1234 *Grimmelmann*, 94 Iowa L. Rev. 1137 (1164), 2008-2009.

1235 Bitkom, https://www.bitkom.org/Publikationen/2013/Studien/Soziale-Netzwerke-dritte-erweiterte-Studie/SozialeNetzwerke-2013.pdf, S. 11, 15.

1236 Bitkom, https://www.bitkom.org/Publikationen/2013/Studien/Soziale-Netzwerke-dritte-erweiterte-Studie/SozialeNetzwerke-2013.pdf, S. 24 ff.

1237 So auch *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 14; *Kutscha*, GR-Schutz im Internet, S. 11, 44 f.; *Piltz*, Soziale Netzwerke, S. 3; *Spiecker gen. Döhmann*, K&R 2012, 717 (720); Art. 29 DatSchGruppe, Stellungnahme 15/2011, WP 187, S. 22; *Preibusch*, in: Neumann-Braun/Autenrieth (Hrsg.), Freundschaft und Gemeinschaft im Social Web, S. 278; vgl. auch *Hoffmann-Riem*, Innovation und Recht, S. 627 f.; vgl. allgemein zum Einfluss sozialen Drucks auf das Verhalten Einzelner: *Thaler/Sunstein*, Nudge, S. 79 ff.; *Wolff*, RW 2015, 194 (201 f.).

1238 So wohl *Rogosch*, Die Einwilligung im Datenschutzrecht, S. 86.

1239 *Simitis*, in: Simitis, BDSG, § 4a Rn. 63 m.w.N.; *Taeger*, in: Taeger/Gabel, § 4a BDSG, Rn. 59; *Buchner*, Informationelle Selbstbestimmung, S. 104 ff.; *Bäcker*, Der Staat (51) 2012, 91 (108); vgl. auch Art. 29 DatSchGruppe, Stellungnahme 15/2011, WP 187, S. 15 ff.; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 78 f., 108 f. plädiert für ergänzende restriktive Kritieren, beispielsweise ob eine gleichwertige Leistung nur unter unzumutbaren Bedingungen zu erlangen ist.

In Bezug auf Facebook sind dabei zwei verschiedene Bereiche zu unterscheiden: Zum einen geht es um die Einwilligung in die Verarbeitung von Daten durch Facebook aus Drittquellen wie etwa dem Messengerdienst Whatsapp, Social PlugIns auf anderen Webseiten oder dem Netzwerk Instagramm. Zum anderen geht es um die Einwilligung in die Datenverarbeitung für die Nutzung des sozialen Netzwerks Facebook im engeren Sinne.

Hinsichtlich der ersten Konstellation hat das Bundeskartellamt am 2. März 2016 ein Verfahren gegen die *Facebook Inc.*, *Facebook Ireland Ltd.* und *Facebook Germany Germany GmbH* eingeleitet, weil insoweit Anhaltspunkte für einen Missbrauch einer marktbeherrschenden Stellung existierten.[1240] In einer vorläufigen Einschätzung bejahte das Bundeskartellamt jüngst einen Missbrauch der marktbeherrschenden Stellung Facebooks hinsichtlich der Sammlung und Verwendung von Nutzerdaten aus Drittquellen, ließ dies für die Datenverarbeitung innerhalb des sozialen Netzwerks Facebook selbst aber ausdrücklich offen.[1241]

Im Fokus der nachfolgenden Betrachtung soll lediglich die zweite Konstellation stehen, also die Vereinbarkeit der Einwilligung in die Datenverarbeitung für die konkrete Nutzung sozialer Netzwerke, insbesondere Facebooks, mit dem Kopplungsverbot. Eine detaillierte Betrachtung der weitergehenden, Drittquellen umfassenden Konstellation, die im Fokus der Untersuchung des Bundeskartellamts steht, würde den Rahmen dieser Arbeit sprengen.

Als Ausgangspunkt lässt sich fragen, ob das Kopplungsverbot überhaupt grundsätzlich auf soziale Netzwerke anwendbar ist. Diese Anwendbarkeit erscheint zunächst problematisch, da die Zwecke der Nutzung und damit auch die Zwecke des mit dem Anbieter bestehenden Vertragsverhältnisses sehr vielfältig sein können. Entsprechend könnte es Probleme bereiten, genau zu definieren, welche Informationen für die Erfüllung des eigentlich Vertragszwecks nicht erforderlich sind. Denn selbst wenn man den Zweck der sozialen Netzwerke nutzerfreundlich auf die private Kontakt- und Interessenpflege beschränkte, ließe sich durchaus argumentieren, dass die Erstellung ausführlicher Persönlichkeitsprofile der Nutzer notwendig ist, um diesen Zweck zu erfüllen und ihnen ein möglichst passgenaues Nutzungserlebnis zu ermöglichen; dies umfasst freilich noch nicht die Nutzung zu Werbezwecken. Allerdings dient die Erstellung von Profilen und deren Verkauf an Werbepartner der Finanzierung des sozialen Netzwerks. Erst sie ermöglichen es überhaupt, das Netzwerk formal ‚kostenlos' zu betreiben.

[1240] http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568.

[1241] http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2017/19_12_2017_Facebook.pdf?__blob=publicationFile&v=3.

Insoweit kann man natürlich überlegen, ob der Slogan „Facebook ist und bleibt kostenlos“[1242] eine irreführende, gar täuschende Werbung darstellt, wenn die Nutzer doch tatsächlich mit ihren Daten bezahlen.[1243] Aber als maßgebliche Finanzierungsquelle steht die Nutzung zu Werbezwecken jedenfalls in einem gewissen Zusammenhang mit dem Zweck der Nutzung.

§ 28 Abs. 3b BDSG verbietet indes ausdrücklich die Kopplung der Erbringung einer Leistung an die Einwilligung in eine Verarbeitung der Daten zu Werbezwecken oder des Adresshandels. Dasselbe gilt nach Art. 7 Abs. 4 DS-GVO, da eine solche Verarbeitung für die Erbringung der Dienstleistung des sozialen Netzwerks angesichts alternativer Finanzierungsmethoden nicht unbedingt notwendig ist. Es wäre widersinnig, wenn das Kopplungsverbot alleine dadurch umgangen werden könnte, dass der Umfang und die Bedeutung der Werbung vergrößert würden und damit über klassische Formen der Werbung und des Adresshandels hinausgingen. Das Kopplungsverbot muss daher auch dann gelten, wenn Werbung das gesamte Angebot finanziert und die Einwilligung damit quasi eine Art von *essentialia negotii* wird, indem sie das Nutzungsentgelt ersetzt.

Dennoch ist ein Verstoß gegen das Kopplungsverbot hinsichtlich der Nutzung des sozialen Netzwerks – jedenfalls zum gegenwärtigen Zeitpunkt – im Ergebnis abzulehnen, da die Dienstleistungen entsprechender sozialer Netzwerke, insbesondere Facebooks, derzeit nicht hinreichend einzigartig und exklusiv sind. Der Wert eines sozialen Netzwerks bemisst sich für den Nutzer natürlich auch an der Zahl der anderen Mitglieder, ein Fakt, der soziale Netzwerke prinzipiell zu hervorragenden Kandidaten für natürliche Monopole macht.[1244] Entsprechend ist Facebook überaus attraktiv und nützlich für Nutzer, denen es auf eine möglichst große Vernetzung mit anderen Nutzern ankommt. Allerdings ist es zu eng betrachtet, die besondere Leistung sozialer Netzwerke ausschließlich auf den Reichweitenaspekt zu verengen. Sie dienen darüber hinaus auch der Selbstdarstellung, dem Austausch mit bekannten Freunden, dem Teilen von Bildern mit diesen und dem Organisieren von Veranstaltungen und Informationen. Für diese Zwecke sind die Leistungen von Facebook und vergleichbaren Anbietern mit ähnlichen Datenschutzbestimmungen aber gerade nicht exklusiv: Immer wieder werden Versuche

[1242] https://de-de.facebook.com/.

[1243] Vgl. *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 47; *Caspar*¸ ZD 2015, 12 (13); vgl. zur ökonomischen Relevanz der Gegenleistung der Daten auch *Hoffmann-Riem*, AöR 2012, 509 (536); *Buchner*, Informationelle Selbstbestimmung, S. 183 ff.; *Newman*, 40 William Mitchell L. Rev., 849 (860 ff.), 2013-2014.

[1244] *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 142 f.; *Spiecker gen. Döhmann*, K&R 2012, 717 (718); *Neuberger*, in: Neuberger/Gehrau (Hrsg.), Soziale Netzwerke, S. 47; vgl. auch *v. Lewinsky*, Matrix des Datenschutzes, S. 58; *Buchholtz*, AöR 2015, 121 (126); *Rogosch*, Die Einwilligung im Datenschutzrecht, S. 86 f.; *Hoffmann-Riem*, Innovation und Recht, S. 638 f.

unternommen, sogar anonyme und gänzlich werbefreie soziale Netzwerke zu etablieren.[1245] Zwar sind diese Netzwerke aufgrund der deutlich geringeren Mitgliederzahl für viele Zwecke weniger attraktiv als Facebook. Anders als beispielsweise im insoweit wegweisenden Urteil zur Schweigepflichtentbindung[1246] existieren aber immerhin (noch) reale Alternativen.[1247] Deren geringere Attraktivität aufgrund des kleineren Netzwerksresultiert im Ergebnisnicht aus der Exklusivität Facebooks, sondern aus der eigenverantwortlichen Entscheidung anderer Nutzer.

Insofern bleibt es jedem vorbehalten, angesichts der existierenden Alternativen seine Freunde davon zu überzeugen, zusammen in ein anderes Netzwerk zu wechseln. Das Kopplungsverbot sollte nicht dahingehend überdehnt werden, dass es den Einzelnen auch vor einer subjektiv als unvernünftig wahrgenommen Wahl eines sozialen Netzwerks seiner Freunde schützen soll. Der Nutzen eines größeren sozialen Netzwerks wird bei Facebook durch die Preisgabe eigener Daten erkauft. Ein Zugang zu Alternativen, welche ebenfalls die grundlegenden Funktionen eines sozialen Netzwerks bieten, insbesondere die Möglichkeiten der digitalen Selbstdarstellung, ist grundsätzlich gegeben. Auch eine Kommunikation mit Freunden ist möglich – beispielsweise klassisch per Telefon oder per datenschutzfreundlicher Messengergruppe –, ohne sich bei Facebook oder einem vergleichbar großen sozialen Netzwerk zu registrieren. Es ist insofern möglich, eine gleichwertige vertragliche Leistung in zumutbarer Weise zu erhalten, auch wenn dies mit etwas mehr Aufwand verbunden sein mag und die Nutzung verschiedener Plattformen erfordern kann, wenn der Einzelne seine Kontakte nicht von einem Wechsel in ein insgesamt datenschutzfreundlicheres Netzwerk überzeugen kann. Ein Verstoß gegen das Kopplungsverbot liegt somit nicht vor, soweit die Nutzung des sozialen Netzwerks Facebook im engeren Sinne betroffen ist.[1248] Diese Einschätzung steht selbstverständlich – wie soeben bereits betont – unter dem Vorbehalt, dass es weiterhin reale Alternativen zur Nutzung von Facebook gibt und Facebook nicht zukünftig eine marktbeherrschende Stellung im Bereich des Angebots sozialer Netzwerke zukommt und die Nutzung sozialer Netzwerke gesellschaftlich weitgehend unverzichtbar wird.

Aus der Tendenz von erfolgreichen sozialen Netzwerken zu natürlichen Monopolen resultieren allerdings in jedem Fall verstärkte staatliche Schutzpflichten, um ein bestehendes

[1245] Ein Beispiel hierfür ist z.B. das Netzwerk www.ello.co.

[1246] BVerfGK 9, 353 (358 ff.) - Schweigepflichtentbindung.

[1247] Alternativen zu Facebook sind beispielsweise das derzeit insbesondere unter jüngeren Nutzern beliebte Snapchat sowie im beruflichen Bereich beispielsweise die sozialen Netzwerke LinkedIn oder Xing.

[1248] Für eine entsprechend restriktive Auslegung des Kopplungsverbots auch bereits *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 78, 108 f.; in diese Richtung auch *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner, S. 432; a.A. wohl *Rogosch*, Die Einwilligung im Datenschutzrecht, S. 86 f.

Machtungleichgewicht zwischen Anbietern, Nutzern und anderen Wettbewerbern auszugleichen und Nutzer verstärkt über die Risiken für ihre informationelle Selbstbestimmung aufzuklären.[1249]

c) Zwischenergebnis

Auch wenn ein Verstoß gegen das Kopplungsverbot hinsichtlich der Einwilligung in die Datenverarbeitung für die Nutzung des sozialen Netzwerks Facebook derzeit abzulehnen ist, bleiben gewichtige Zweifel an der generellen Geeignetheit der Einwilligung als regulatorisches Instrument in Bezug auf soziale Netzwerke. Sowohl die hinreichende Informiertheit, als auch die Freiwilligkeit und Bestimmtheit der Einwilligung laufen Gefahr, zu bloßen Floskeln und Fiktionen zu verkommen. Andererseits dürfte aber auch klar sein, dass es dem Grundrecht auf informationelle Selbstbestimmung einen Bärendienst erwiese, die Einwilligung für völlig untauglich zu erklären und zugunsten von abschließenden gesetzlichen Regeln abzuschaffen: Dieser Schritt würde zwar das Problem einer möglichen Fiktion der Einwilligung beseitigen. Allerdings geschähe es um den Preis, die individuelle Freiheit zur selbstbestimmten Informationspreisgabe weitgehend zu verbieten und sähe sich daher erheblichen verfassungsrechtlichen Bedenken ausgesetzt.[1250]

Entsprechend lässt sich festhalten, dass die Einwilligung in die Datenverarbeitung bei Facebook jedenfalls in ihrer aktuellen Fassung in den Datenrichtlinien die Anforderungen der §§ 4a Abs. 1 BDSG, 13 Abs. 1 TMG und zukünftig Art. 7 DS-GVO nicht vollumfassend erfüllt. Es erscheint auch höchst zweifelhaft, dass eine wirksame Einwilligung überhaupt ohne unterstützende Maßnahmen möglich ist, da eine hinreichend effektive Aufklärung über Zwecke und Schritte der Datenverarbeitung angesichts des möglichen Umfangs wohl nur schwer erfolgen kann. Anstatt deswegen aber gleich die Einwilligung inklusive des gesamten Konzepts des Verbots mit Erlaubnisvorbehalt im Datenschutzrecht gänzlich zu beerdigen[1251], sollten

[1249] *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 142 f.; *Bäcker*, Der Staat (51) 2012, 91 (105 ff.); vgl. auch *Kühling*, Die Verwaltung (44) 2011, 525 (551); ein Überblick über mögliche Maßnahmen soll sogleich im nächsten Abschnitt unter D.III.3.a) erfolgen.

[1250] *Spindler*, GRUR-Beilage 2014, 101 (102); *ders.*, Gutachten F zum 69. dt. Juristentag, 2012, S. 99; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 90; *Sandfuchs*, Privatheit wider Willen, S. 165 ff.; zur freiheitsbeschränkenden Wirkung solcher paternalistischer Maßnahmen auch noch unten unter D.III.4.a).

[1251] So *Härting*, NJW 2013, 2065 (2070); *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 90.

technische und rechtliche Alternativen implementiert werden, die diese ergänzen und unterstützen.[1252]

3. Selbstdatenschutz und „Risk-Based Approach“

Es existieren verschiedene Konzepte, um die strukturellen Defizite der Einwilligung und die existierenden Macht- und Informationsfälle in sozialen Netzwerken auszugleichen. Hierzu zählen insbesondere der Selbstdatenschutz sowie in den letzten Jahren verstärkt auch der „Risk-Based Approach“. Beiden Ansätzen ist gemein, dass sie insbesondere die Überforderung des Nutzers mindern wollen, die die Einwilligung, wie soeben dargelegt, bedeuten kann.

a) Selbstdatenschutz in sozialen Netzwerken

Der Selbstdatenschutz steht in engem Zusammenhang mit der Annahme einer staatlichen Infrastrukturverantwortung für die Gewährleistung sicherer Kommunikation und Informationspreisgabe, die aus der staatlichen Schutzpflicht für die informationelle Selbstbestimmung folgt.[1253] Ausgehend davon, dass in der globalisierten Welt ubiquitärer Datenverarbeitung ein rein staatlicher Datenschutz nicht mehr geleistet werden kann, soll der individuelle Nutzer durch technische Hilfsmittel sowie entsprechende rechtliche Rahmenbedingungen und Infrastrukturleistungen in die Lage versetzt werden, selbstbestimmt über die eigenen Daten zu verfügen.[1254] Hierbei ist insbesondere an die im Folgenden diskutierten Instrumente zu denken.

aa) Anwendung der Grundprinzipien des Datenschutzrechts als Elemente eines Selbstdatenschutzes

Viele der bisher analysierten Regelungen im Datenschutzrecht in Bezug auf soziale Netzwerke lassen sich auch als Elemente des Selbstdatenschutzes einzustufen.[1255] Dies gilt insbesondere

---

[1252] So auch *Spindler*, GRUR-Beilage 2014, 101 (103) m.w.N.; *ders.*, Gutachten F zum 69. dt. Juristentag, 2012, S. 100; *Bäcker*, Der Staat (51) 2012, 91 (113 ff.); *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 35 ff.; vgl. *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 33; *Sandfuchs*, Privatheit wider Willen, S. 132 ff.

[1253] Instruktiv: *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 36 ff.; vgl. auch *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 143 f.; *Sandfuchs*, Privatheit wider Willen, S. 132 ff.; *Buchner*, Informationelle Selbstbestimmung, S. 118 ff.; *Hoffmann-Riem*, AöR 1998, 513 (534 ff.); *Gurlit*, NJW 2010, 1035 (1040 f.).

[1254] *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 3 f., 36; *Ders./Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 150 ff.; Art. 29 DatSchGruppe, Stellungnahme WP 227, S. 3; *Bäcker*, Der Staat (51) 2012, 91 (111 ff.); *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, S. 590 f.; *v. Lewinsky*, Matrix des Datenschutzes, S. 66; *Hoffmann-Riem*, AöR 1998, 513 (532).

[1255] *v. Lewinsky*, Matrix des Datenschutzes, S. 66; *Sandfuchs*, Privatheit wider Willen, S. 133 ff.; *Bäcker*, Der Staat (51) 2012, 91 (114); *Hoffmann-Riem*, AöR 1998, 513 (535 f.).

für die engen Zweckbindungsregelungen, aber auch die Betroffenenrechte der §§ 33 ff. BDSG bzw. Art. 12 ff. DS-GVO. Zwar geht das Datenschutzrecht im Prinzip von einem dichotomen Verhältnis von Datenverarbeiter und Betroffenem aus. Wie oben unter D.I.3 gezeigt wurde, sind die gesetzlichen Regelungen aber flexibel genug, um mit den verschiedenen Akteuren in sozialen Netzwerken umzugehen. Anbieter, Nutzer sowie Betreiber von Fanpages, Social PlugIns und sonstigen Angeboten erweisen sich in unterschiedlichem Maße als Verantwortliche für Datenverarbeitungen und damit als Adressaten datenschutzrechtlicher Regelungen. Betroffenen stehen umfassende Auskunfts- und Löschungsrechte gegen die Verantwortlichen zu, die ihrerseits gegebenenfalls Benachrichtigungspflichten gemäß § 33 BDSG bzw. Art. 13 f. DS-GVO unterliegen.

Auch ein Recht auf anonyme bzw. pseudonyme Nutzung ist in § 13 Abs. 6 TMG normiert. Wie unter C.II gezeigt wurde, ist mit den überzeugenderen Argumenten davon auszugehen, dass dieses Recht insbesondere im Fall Facebooks bisher kollisionsrechtlich Anwendung findet und daher zu beachten ist. Wie ebenfalls gezeigt wurde, enthält die DS-GVO zwar kein ausdrückliches entsprechendes Recht. Angesichts der aus ihm resultierenden Vermeidbarkeit des Personenbezugs jedenfalls gegenüber anderen Nutzern des sozialen Netzwerks bleibt aber zu hoffen, dass dieses Recht zukünftig aus den Vorschriften der Art. 25 und 32 DS-GVO abgeleitet werden wird.[1256] Die Möglichkeit der pseudonymen Nutzung stellt ein wesentliches Element des Selbstschutzes dar[1257], das entsprechend auch vom Staat durchgesetzt werden sollte.[1258]

Mit den Grundsätzen der Zweckbindung in §§ 28 Abs. 1 S. 2, 4 Abs. 4 S. 1 Nr. 2 BDSG und § 13 Abs. 1 TMG sowie der Datenvermeidung und Datensparsamkeit gemäß § 3a BDSG existieren wichtige gesetzliche Rahmenbedingungen, die den Einzelnen befähigen, eine informierte Abwägung darüber zu treffen, welche Daten er zu welchen Zwecken preisgibt. Sie sichern damit die informationelle Selbstbestimmung ab und helfen, sie in der Rechtspraxis zu schützen.[1259] Insoweit ist sehr zu begrüßen, dass Art. 5 Abs. 1 DS-GVO diese Grundsätze

[1256] Hierzu bereits oben unter D.II.2.a).

[1257] *Caspar*, ZRP 2015, 233 (235); *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 56 ff.; *Nietsch*, Anonymität, S. 39 f.; vgl. auch allgemein für Big Data Techniken *Martini*, DVBl. 2014, 1481 (1487); *Weichert*, ZD 2013, 251 (258 f.).

[1258] Die einstweilige Anordnung gemäß § 38 Abs. 5 BDSG des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gegen Facebook vom Juli 2015, den rechtswidrigen Klarnamenzwang für Nutzerprofile in den Nutzungsbedingungen aufzuheben, ist daher sehr zu begrüßen.

[1259] *v. Lewinsky*, Matrix des Datenschutzes, S. 58; *Martini*, DVBl. 2014, 1481 (1487); *Weichert*, ZD 2013, 251 (254); *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 71 ff.

weitgehend übernimmt.[1260] Allerdings ist es der Vereinheitlichung der bisher bereichsspezifischen Erlaubnistatbestände für die Datenverarbeitung in dem weit gefassten Art. 6 DS-GVO immanent, dass die spezifische Zweckbindung einer einzelnen Datenverarbeitung leidet.[1261] Ob dies durch die nach Art. 13 f. DS-GVO normierten Informationspflichten bezüglich der verfolgten Zwecke aufgefangen werden kann, bleibt abzuwarten. Angesichts der oben beschriebenen Probleme in Bezug auf die Informiertheit einer Einwilligung[1262] ist dies jedenfalls fraglich.[1263]

Mit Vorsicht wird zudem zu beobachten sein, wie die Praxis die Vorschrift des Art. 6 Abs. 4 DS-GVO anwenden wird, der eine Verarbeitung von Daten auch zu anderen Zwecken erlaubt als zu den ursprünglichen, sofern diese neuen Zwecke mit den alten „vereinbar" sind. Diese Vorschrift dient sichtlich der Stärkung der Möglichkeiten einer Big-Data Auswertung von Daten; ebensolche Auswertungen können aber, wie oben beschrieben wurde, die informationelle Selbstbestimmung Betroffener erheblich gefährden.[1264] Während Art. 6 Abs. 4 lit d) DS-GVO zwar vorschreibt, die möglichen Folgen der Verarbeitung mit in die Vereinbarkeitsabwägung aufzunehmen, bleibt abzuwarten, wie streng diese Vorschrift ausgelegt werden wird. Die Artikel-29 Datenschutzgruppe warnt insoweit sehr zutreffend davor, dass der gesamtgesellschaftliche Nutzen von umfassenden Big-Data Auswertungen noch nicht belegt ist und, selbst wenn er erwiesen wäre, eine wirtschaftliche Nutzung von Daten stets unter der Prämisse erfolgen muss, dass die Menschen- und Grundrechte europäischer Bürger gewahrt werden.[1265] Persönliche Daten dürfen nicht ausschließlich als ökonomische Ressource betrachtet werden und die bloße technische Machbarkeit und ein diffuser Nutzen für die Gesellschaft den individuellen Persönlichkeitsschutz nicht pauschal aushebeln.[1266]

Die teilweise seit Jahrzehnten etablierten Grundprinzipien des Datenschutzrechts erweisen sich damit auch in der Zeit ubiquitärer Datenverarbeitung in mehrseitigen Rechtsbeziehungen als wichtige und effektive Elemente zur Gewährleistung eines Selbstdatenschutzes. Es bleibt zu hoffen, dass dies auch unter der DS-GVO geltende Rechtspraxis bleiben wird.

[1260] Hierzu *Dammann*, ZD 2016, 307 (311 f.).
[1261] *Nebel/Richter*, ZD 2012, 407 (409).
[1262] Oben unter D.III.2.b)aa).
[1263] Kritisch auch *Keppeler*, MMR 2015, 779 (781).
[1264] Vgl. oben unter B.II.3.b)bb); eine stärkere Betonung der Zweckvereinbarkeit zulasten der strengen Zweckbindung befürwortete dagegen bereits *Eifert*, Zweckvereinbarkeit, in: Gropp u.a. (Hrsg.), S. 143 ff., um übermäßiger Verrechtlichung zu entgehen.
[1265] Art. 29 DatSchGruppe, Stellungnahme WP 221, S. 2 f.;
[1266] Art. 29 DatSchGruppe, Stellungnahme WP 227, S. 2; *Martini*, DVBl. 2014, 1481 (1483).

bb) Datenschutz durch Technik und Design

Datenschutz durch Technik bzw. Privacy by Design verfolgt den Ansatz, den Persönlichkeitsschutz durch technische Vorkehrungen sicherzustellen, indem IT-Systeme von vorneherein datenschutzkonform und im Zweifel datensparsam gestaltet werden.[1267] Datenschutzrechtliche Belange werden damit nicht nur auf der Ebene des Datenverarbeiters relevant, sondern können auch auf die Herstellerebene vorverlagert werden, indem bereits für die Herstellung von Produkten und IT-Systemen eine Pflicht zur Berücksichtigung von Datenschutzaspekten statuiert wird. Dies erleichtert die Regulierung und Kontrolle der Einhaltung von Datenschutzbelangen, da bei weniger Akteuren angesetzt wird.[1268] Es handelt sich daher insgesamt um ein zu begrüßendes, sehr zeitgemäßes Konzept.

Deutlicher als bisher bestehende Regelungen u.a. in § 9 BDSG normiert Art. 25 DS-GVO, dass bei jedem Stadium der Datenverarbeitung technische und organisatorische Maßnahmen getroffen werden sollen, die die Einhaltung der vorgeschriebenen Datenschutzregeln sicherstellen. Während der ursprüngliche Entwurf der Kommission zu Recht als wenig mehr als ein „bloßer Programmsatz" kritisiert wurde[1269], konkretisierte der *LIBE*-Entwurf zumindest die Anforderungen und strich Konkretisierungsermächtigungen der Kommission. Dennoch muss man der Regelung auch in ihrer Endfassung vorhalten, dass sie sehr vage bleibt und sich damit unter Umständen als eher durchsetzungsschwach erweisen wird.[1270] Dadurch, dass insbesondere keine ausdrückliche Vorgaben für die Hersteller von IT-Systemen gemacht werden, sondern wie bisher nur Pflichten für die konkreten Datenverarbeiter statuiert werden,

[1267] *Heckmann*, NJW 2012, 2631 (2634); *Piltz*, Soziale Netzwerke, S. 292 ff.; *Maisch*, Informationelle Selbstbestimmung, S. 246 ff.; instruktiv: *Roßnagel*, in: ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 44 ff.

[1268] Vgl. *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 122 ff.; *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 46 f.

[1269] *Roßnagel/Kroschwald*, ZD 2014, 495 (499); vgl. auch *Sydow/Kring*, ZD 2014, 271 (273); *Hornung*, ZD 2012, 99 (103); *Heckmann*, NJW 2012, 2631 (2634).

[1270] Kritisch insoweit *Roßnagel/Kroschwald*, ZD 2014, 495 (499); *Heckmann*, NJW 2012, 2631 (2634); *Koós/Englisch*, ZD 2014, 276 (280). Art. 23 Abs. 1a des *LIBE*-Entwurfs hatte noch vorgesehen, Privacy by Design zur Voraussetzung bei der Auftragsvergabe in bestimmten öffentlichen Vergabeverfahren zu machen. Diese Voraussetzung wurde indes vom Ratsentwurf nicht übernommen und auch in der endgültigen Fassung gestrichen. Während diese Vorschrift jedenfalls im öffentlich-rechtlichen Bereich die Durchsetzung hätte verbessern können, hätte sie freilich keine Verbesserung im Rahmen rein privater IT-Anwendungen bedeutet.

verschenkt der Entwurf ein erhebliches Potential, das grundsätzlich in dem Ansatz des Datenschutzes durch Technik steckt.[1271]

Datenschutz durch Technik und Privacy by Design sind gerade für soziale Netzwerke sehr begrüßenswerte Maßnahmen. Probleme hinsichtlich der informationellen Selbstbestimmung resultieren nicht zuletzt daraus, dass viele Nutzer die Vorteile einer Mitgliedschaft im sozialen Netzwerk vorschnell überbewerten und sich nicht hinreichend mit potentiellen Risiken auseinandersetzen.[1272] Datenschutzfreundliche Grundeinstellungen, die Risiken minimieren, kämen ihnen daher besonders zu Gute. Indem derartige Grundeinstellungen Komplexität technisch reduzieren, sind sie zudem gut geeignet, der Überforderung von Nutzern bei umfangreichen Datenschutzbestimmungen im Rahmen der Einwilligungserklärung zu begegnen.[1273] Im Folgenden sollen einige ausgewählte Beispiele für Datenschutz durch Technik in sozialen Netzwerken analysiert werden.[1274]

i) Zeitliche Beschränkung der Wirksamkeit der Einwilligung

Die auf Langfristigkeit angelegte Mitgliedschaft in sozialen Netzwerken bringt es mit sich, dass sich Nutzer nach einer einmaligen Anmeldung nicht mehr ausführlich mit sich ändernden Datenschutzbedingungen auseinandersetzen, sondern sich vielmehr an die Nutzung des sozialen Netzwerks gewöhnen und hierüber trotz möglicherweise geänderter persönlicher Einstellungen zum Datenschutz nicht mehr reflektieren.[1275] Hierbei ist auch an faktisch stillgelegte Accounts zu denken, die nicht mehr genutzt werden, für die sich die Nutzer aber auch zu wenig interessieren, um sie noch formal zu löschen. Das rechtliche Fortbestehen der ursprünglich erteilten Einwilligung ermöglicht es den Betreibern, die Daten trotz der fehlenden Nutzeraktivität weiter zu verwenden. Dies kann insbesondere dann zu einem Problem werden,

---

[1271] *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 144 f.; *Barlag*, in: Roßnagel (Hrsg.), Europäische DS-GVO, § 3 Rn. 249. kritisch auch *Heckmann*, NJW 2012, 2631 (2634); vgl. zur Regelsetzung durch technische Standards und Voreinstellungen *Hoffmann-Riem*, AöR 2012, 509 (532 f.); vgl. grundlegend auch *Lessig*, Code is Law, http://www.harvardmagazine.com/2000/01/code-is-law-html.

[1272] Hierzu bereits oben unter D.III.2.b); vgl. auch *Heckmann*, NJW 2012, 2631 (2633 f.); *Piltz*, Soziale Netzwerke, S.292 ff.; *Grimmelmann*, 94 Iowa L.Rev. 1137 (1151 ff.), 2008-2009.

[1273] *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 145; *Heckmann*, NJW 2012, 2631 (2634); *Von der Lühe*, Perspektive der Nutzer, in: Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co, S. 70; vgl. auch *Spindler*, GRUR-Beilage 2014, 101 (103); *Buchholtz*, AöR 2015, 121 (148); *Masing*, NJW 2012, 2305 (2308 f.); *Bäcker*, Der Staat (51) 2012, 91 (113 f.); vgl. auch *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 47.

[1274] Weitere, von *Maisch*, Informationelle Selbstbestimmung, S. 331 ff. diskutierte Maßnahmen umfassen beispielsweise eine sichere Authentifikation bei der Anmeldung und Nutzung, den Schutz vor rechtswidriger Vervielfältigung von Bildern und den Schutz vor Identitätsdiebstahl.

[1275] Vgl. Art. 29 DatSchGruppe, Stellungnahme 15/2011, WP 187, S. 24; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 79, 109 f.; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 373 ff.

wenn der Eigentümer des sozialen Netzwerks sich ändert und damit gegebenenfalls auch die Person des Datenverarbeiters. Natürlich könnte man es in die Verantwortung der Nutzer verweisen, hier aktiv einer Zweckentfremdung ihrer Daten vorzubeugen und sich gegebenenfalls um eine Löschung zu bemühen. Tatsächlich ist ein solches Tätigwerden der Nutzer aber wenig realistisch.[1276]

Eine mögliche Lösung ist ein technisches ‚Verfallsdatum' der Einwilligung.[1277] Nach einer vorher festgelegten Dauer (z.B. mehrere Monate oder auch mehrere Jahre) soll der Nutzer aufgefordert werden, seine Einwilligung erneut abzugeben. Verweigert er diese, gilt die Einwilligung als erloschen und eine weitere Datenverarbeitung wird damit unzulässig. Technisch ist diese Lösung durchaus umsetzbar[1278] und sie bietet auch eine relativ hohe Rechtssicherheit sowohl für den Anbieter als auch den Nutzer sozialer Netzwerke. Im Ergebnis wäre es eine regelmäßige Aufforderung zu einem neuen ‚Opt-In'.

Eine Spielart dieses Modells wäre eine regelmäßige Nachfrage, ob ein Nutzer noch ein Mitglied sein will oder seinen Account löschen lassen möchte, insbesondere wenn schon seit langem keine Aktivität in seinem Profil mehr feststellbar war.[1279] Hierdurch würde der Nutzer zumindest regelmäßig mit der Frage konfrontiert, ob er seine Einwilligung aufrechterhalten oder diese zurückziehen will. Im Kern handelt es sich damit um eine Erinnerung an ein mögliches ‚Opt-Out'. Angesichts der Notwendigkeit eines zusätzlichen Tätigwerdens des Nutzers zur Aufhebung der Einwilligung ist indes wie effektiv dieses Modell letzten Endes wäre: Aufgrund von verhaltensökonomisch zu beobachtenden Effekten wie individueller Verlustaversion und des Status Quo Bias[1280] steht zu erwarten, dass weniger Nutzer von dieser Möglichkeit Gebrauch machen würden, auch wenn sie ein soziales Netzwerk eigentlich nicht mehr nutzen.

[1276] *Mayer-Schönberger*; Die Tugend des Vegessens, S.84 ff. legt ausführlich und überzeugend dar, wie u.a. durch die Verbilligung von Speichermedien eine „Ökonomie des Speicherns" entstanden ist, welche das Löschen und damit Vergessen von Informationen unverhältnismäßig teuer in Form von Opportunitätskosten macht, was zu immer seltenerem Löschen von Informationen führt.

[1277] *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 145; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 109; *Piltz*, Soziale Netzwerke, S. 288 ff.; *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107).

[1278] Vgl. *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107).

[1279] Art. 29 DatSchGruppe, Stellungnahme 15/2011, WP 187, S. 24; vgl. auch *Radlanski*, Das Konzept der Einwilligung, S. 214 f.; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 374.

[1280] Der Status Quo Bias beschreibt eine verhaltensökonomisch nachweisbare Tendenz von Menschen, in ihrer gegenwärtigen Situation zu verharren und beispielsweise nicht den Anbieter einer Leistung zu wechseln oder einen nicht mehr genutzten Vertrag zu kündigen, weil der Schritt zur Veränderung subjektiv als zu großer Aufwand empfunden wird. Instruktiv: *Sunstein/Thaler*, Nudge, S. 53 ff.; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 263 ff.; *Wolff*, RW 2015, 194 (199 ff.).

Teilweise wird auch vertreten, dass die Wirksamkeit der Einwilligung jedenfalls in Fällen faktisch stillgelegter Accounts nach dem Verstreichen von mehreren Jahren von selbst erlischt, da sie sich auf andere Umstände bezogen habe, selbst wenn sie einst für eine unspezifizierte Dauer abgegeben wurde.[1281] Dies ist *de lege lata* fragwürdig, da eine Einwilligung bei unveränderten Verhältnissen durchaus von unbegrenzter Dauer gültig sein kann.[1282] Es wäre daher abhängig vom Einzelfall, ob eine hinreichende Veränderung der Verhältnisse vorliegt. Diese Abgrenzung würde aber – in Ermangelung klarer gesetzlicher Regeln – zu erheblicher Rechtsunsicherheit für die Diensteanbieter führen. Die Möglichkeit einer technischen Beschränkung der Einwilligung mit einem gleichsam eingebauten Verfallsdatum wäre daher vorzugswürdig.

ii) Der digitale Radiergummi: Ein Recht auf Vergessenwerden?

Einen anderen Ansatz, der in seiner Bedeutung weit über soziale Netzwerke hinausreicht, verfolgen Überlegungen zu einem allgemeinen „digitalen Radiergummi", mit dem Internetnutzern ermöglicht werden soll, ihre Spuren im Internet zu tilgen bzw. mit einem automatischen „Verfallsdatum" zu versehen.[1283] Diskussionen hierüber sind eng verknüpft mit der breiteren Diskussion um ein ‚Recht auf Vergessenwerden' im Internet.[1284] Für soziale Netzwerke entfalten diese Überlegungen insoweit Bedeutung, als sie die Möglichkeit implizieren, die dort getätigten Spuren umfassend löschen zu lassen.[1285] Freilich sind Löschungsrechte im Grundsatz seit Jahrzehnten in den Datenschutzgesetzen normiert, nicht zuletzt in Art. 12 lit.b) DSRL bzw. in § 33 Abs. 2 BDSG und §§ 13 Abs. 4 S. 1 Nr. 2, 15 Abs. 8 TMG. Diese setzen aber stets voraus, dass sich der Betroffene direkt an die verantwortliche

---

1281 *Zimmermann*, Einwilligung im Internet, S. 269.

1282 *Gola/Schomerus*, § 4a BDSG, Rn. 32a; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 79.

1283 Grundlegend: *Mayer-Schönberger*, Die Tugend des Vergessens, S. 201 ff.; vgl. auch *SpindlerB*, Gutachten F zum 69. dt. Juristentag, 2012, S.85 ff.; auch die deutsche Bundesregierung unterstützte die Idee eines solchen „digitalen Radiergummis", bzw. eines „Verfallsdatums" von Daten im Internet, vgl. http://www.heise.de/newsticker/meldung/Aigner-Hoechster-Datenschutz-made-in-Germany-1163613.html, http://www.heise.de/newsticker/meldung/Digitaler-Radiergummi-ist-gestartet-1175979.html; *Von der Lühe*, Perspektive der Nutzer, in: Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co, S. 72; kritisch zur technischen Umsetzbarkeit und Effektivität dagegen *Nolte*, ZRP 2011, 236 (237 f.); *Piltz*, Soziale Netzwerke, S. 287 ff.

1284 *Buchholtz*, AöR 2015, 121 (124 ff.); *Nolte*, NJW 2014, 2238 (2240 f.); *Boehme-Neßler*, NVwZ 2014, 825 (826 ff.); *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 139 ff.; *Hornung/Hofmann*, JZ 2013, 163 (164 ff.); *Nolte*, NJW 2014, 2238 (2240 ff.); *ders.*, ZRP 2011, 236 (236 ff.); vgl. auch *Spindler*, GRUR-Beilage 2014, 101 (105); *ders.*, Gutachten F zum 69. dt. Juristentag, 2012, S. 35 f.; *Masing*, NJW 2012, 2305 (2308); grundlegend zur Bedeutung des Vergessens in der digitalen Zeit: *Mayer-Schönberger*, Die Tugend des Vergessens, S.112 ff.

1285 Da die Daten stets auf fremden Servern gespeichert werden, auf welche die Nutzer keinen eigenen Zugriff haben, kann es hier immer nur um einen Anspruch auf Löschung gehen. Eine eigenhändige Lösung, vergleichbar zu einem „eigenhändigen Radieren" ist technisch ausgeschlossen.

Stelle wendet. Im Zeitalter des Internets, in dem Informationen immer schneller und weiter geteilt werden können, schafft dies schnell eine unübersehbare Anzahl von möglichen Adressaten, an die der Betroffene sich wenden müsste. Die Überlegungen zum „Recht auf Vergessenwerden" haben zum Ziel, diese Menge an Adressaten zu reduzieren und durch ein einfacher auszuübendes Löschungsrecht zu ersetzen.

Mit der Veröffentlichung des Kommissionsentwurfs wurde medienwirksam über das – angeblich – in Art. 17 DS-GVO-E a.F. enthaltene „Recht auf Vergessenwerden" berichtet.[1286] Bei genauerem Hinsehen entpuppte sich dieses vermeintliche neue Recht indes nicht als materieller Löschungsanspruch, sondern lediglich eine Statuierung von Informationspflichten bzw. Pflichten zur Weitergabe des Löschungsbegehrens, die materiell nicht über die bereits bestehenden Regelungen hinausging.[1287] Dies gilt auch für die nunmehr verabschiedete Endfassung: Der Verarbeiter ist gemäß Art. 17 Abs. 1 DS-GVO unter bestimmten Voraussetzungen zur Löschung von Daten verpflichtet, die er selbst gespeichert hat. Bezüglich solcher Daten, die er an Dritte weitergegeben oder veröffentlich hat, besteht gemäß Art. 17 Abs. 2 DS-GVO indes nur eine Pflicht, diese Dritten über das Löschungsbegehen zu informieren. Ob sie einer Löschungsverpflichtung unterliegen, bestimmt sich sodann nach deren eigenen Datenverarbeitungsbefugnissen.[1288] Das konkrete Löschungsbegehren muss zudem von dem Betroffenen gegebenenfalls direkt gegenüber diesen Dritten durchgesetzt werden, da der ursprüngliche Verarbeiter nur der Informationspflicht unterliegt.

Ein deutlich weitergehendes Recht in Form eines echten „digitalen Radiergummis", das für die Datenverarbeitung Verantwortliche verpflichtet hätte, die Löschung der von ihnen veröffentlichten Daten auch im Verantwortungsbereich Dritter sicherzustellen, war zwar in einem vorläufigen Entwurf von November 2011 noch enthalten.[1289] In diesem Umfang ist ein solches Recht indes rein faktisch nicht durchsetzbar, da der Verantwortliche in aller Regel nicht

[1286] Vgl. z.B. FAZ v. 25.1.2012, http://www.faz.net/aktuell/politik/europaeische-union/eu-kommission-will-mehr-datenschutz-ein-recht-auf-vergessen-im-netz-11623455.html; Spiegel Online v. 25.1.2012 http://www.spiegel.de/netzwelt/netzpolitik/informationelle-selbstbestimmung-das-recht-auf-vergessen-und-die-netzfreiheit-a-817830.html; vgl. auch *Nolte*, NJW 2014, 2238 (2240).

[1287] Ausführlich: *Hornung/Hofmann*, JZ 2013, 163 (166 f.); *Buchholtz*, AöR 2015, 121 (134); *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107); *Kipker/Voskamp*, DuD 2012, 737 (741); *Gierschmann*, ZD 2016, 51 (53 f.); *Schantz*, NJW 2016, 1841 (1845).

[1288] *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 141; *Spindler*, GRUR-Beilage 2014, 101 (105).

[1289] Dort in Art. 15, abrufbar unter http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf; vgl. auch *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 141; *ders./Hoffmann*, JZ 2013, 163 (167).

auf die Speicher und Server der Dritten zugreifen kann.[1290] Entsprechend wurde es aus dem endgültigen Kommissionsentwurf entfernt. Im Entwurf des Parlaments wurde ferner die reißerische Bezeichnung als ein „Recht auf Vergessenwerden" als irreführend gestrichen und durch die Bezeichnung als Recht auf Löschung ersetzt. Die endgültige Fassung kombiniert die beiden Bezeichnungen, setzt das „Recht auf Vergessenwerden" aber immerhin relativierend in Anführungsstriche.

Das Löschungsrecht, wie es nunmehr in Art. 17 DS-GVO enthalten ist, erweist sich somit im Ergebnis als wenig effektiv, um dem Betroffenen zu einer umfassenden Löschung seiner Spuren im Internet zu verhelfen. Es stellt eine allenfalls geringfügige Verbesserung gegenüber den bereits geltenden Regeln dar, die in Art. 12 lit. b) u. c) DSRL dem Betroffenen Berichtigungs-, Löschungs- und Sperrungsansprüche gewähren und die verantwortlichen Stellen zur Weiterleitung von Löschungsbegehren an Dritte verpflichten, denen Daten übermittelt wurden.[1291] Angesichts der erheblichen faktischen Probleme ist es indes fraglich, ob eine weitergehende Löschungsverpflichtung überhaupt realistisch wäre. Hilfreicher wäre insoweit auch hier der zuvor beschriebene technische Ansatz, Daten – ähnlich wie bei der Einwilligung – von vorneherein mit einem automatischen Verfallsdatum zu versehen.[1292]

Der dem Recht auf Vergessenwerden zugrundeliegende Anspruch auf Löschung von Daten war ein wichtiger Bestandteil der *Google*-Entscheidung des EuGH im Mai 2014. Der EuGH entschied, dass Suchmaschinenbetreibern eine Pflicht zukommen könne, Links zu ursprünglich rechtmäßig veröffentlichten, wahrheitsgemäßen personenbezogenen Informationen aus der Ergebnisliste zu löschen.[1293] Dies sei insbesondere dann der Fall, wenn „die Informationen in Anbetracht aller Umstände des Einzelfalls den Zwecken der in Rede stehenden Vereinbarung durch den Suchmaschinenbetreiber nicht entsprechen, dafür nicht oder nicht mehr erheblich sind oder darüber hinausgehen" [1294]. Maßgeblich sei eine Abwägung der Interessen des Betroffenen mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers sowie „dem

---

[1290] *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 141 m.w.N.; *ders./Hoffmann*, JZ 2013, 163 (167); *Piltz*, Soziale Netzwerke, S. 287 f.; *Dix*, in: Simitis, BDSG, § 35 Rn. 8; *Däubler*, in: DKWW, § 35, Rn. 3.

[1291] *Spindler*, GRUR-Beilage 2014, 101 (105); *Hornung/Hofmann*, JZ 2013, 163 (165); *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107).

[1292] *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107); grundlegend *Mayer-Schönberger*, Die Tugend des Vergessens, S. 201 ff. Sogar diese Lösung würde freilich dort fehlgehen, wo Dritte Kopien von den Daten machen, die unabhängig von diesem Verfallsdatum sind, notfalls mit Screenshots und im Internet verbreiteten Bildern. Hier bliebe der Betroffene weiterhin auf das mühselige Erwirken einzelner Löschungsverfügungen angewiesen.

[1293] EuGH, *Google Spain*, Rs. C-131/12, Rn. 94 = JZ 2014, 1009 (1016).

[1294] EuGH, *Google Spain*, Rs. C-131/12, Rn. 94 = JZ 2014, 1009 (1016).

Interesse der breiten Öffentlichkeit daran, die Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche zu finden".[1295]

Das Urteil wurde dafür kritisiert, dass die Abwägungsentscheidung zu holzschnittartig dargestellt und zu einer erheblichen Einschränkung der Informationsrechte der Öffentlichkeit führen würde.[1296] Besonders kritisch wurde zudem gesehen, dass Suchmaschinenbetreiber ohne eine weitere Kontrollinstanz Adressaten der Löschpflicht sind, sich also einzelne Betroffene durch gezielte Löschungsanträge Vorteile verschaffen könnten.[1297] Eine angemessene Einzelfallprüfung durch den Suchmaschinenbetreiber sei weder vom Umfang her zu leisten, noch gäbe es Anreize für eine restriktive Handhabung der Löschungsanträge, da im Zweifel Schadensersatzansprüche wegen einer Verletzung des Persönlichkeitsrechts durch eine unterlassene Löschung drohen könnten.[1298] Der Kritik ist grundsätzlich beizupflichten. Die Analyse soll sich im Folgenden jedoch auf die Auswirkungen der Entscheidung auf soziale Netzwerke beschränken.

Dass Individuen grundsätzlich Löschungsrechte zukommen können, ist unstrittig gesetzlich festgelegt. Die besondere Relevanz der Entscheidung des EuGH liegt in der ausdrücklichen Erstreckung dieses Rechts auf ursprünglich rechtmäßig veröffentlichte Daten im gleichsam sekundären Verwendungskontext von Suchmaschinenergebnissen. Der EuGH schafft kein Recht des Betroffenen, die ursprünglich rechtmäßige Veröffentlichung rückgängig zu machen. Er schränkt stattdessen die leichtere Auffindbarkeit der Information sowie ihre Verknüpfung mit anderen Informationen ein. Während die Information damit zwar nicht gelöscht wird, wird ihr Verbreitungsgrad angesichts des enormen Einflusses, den Suchmaschinen auf die Navigation des Internets haben, massiv beschränkt. Zudem wird eine spontane Form der Profilbildung unterbunden, die ansonsten dadurch erfolgt, dass Personen, die lediglich den Namen eines Betroffenen mit einer Suchmaschine recherchieren, sofort auf zugehörige Informationen hingewiesen werden. Diese Zusammenhänge waren dem EuGH nicht nur bewusst; sie stellen sogar die zentrale Begründung für die Schwere der durch das Löschungsrecht beseitigten Grundrechtsbeeinträchtigung bei dem Betroffenen dar.[1299]

[1295] EuGH, *Google Spain*, Rs. C-131/12, Rn. 97 = JZ 2014, 1009 (1016).

[1296] *Masing*, VerfBlog, 2014/8/14, dort unter 6., http://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/; vgl. auch *Buchholtz*, AöR 2015, 121 (143); *Spindler*, JZ 2014, 981 (986 f.); *Boehme-Neßler*, NVwZ 2014, 825 (829 f.).

[1297] *Masing*, VerfBlog, 2014/8/14, dort unter 5., http://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/; *Spindler*, JZ 2014, 981 (987 f.).

[1298] *Masing*, VerfBlog, 2014/8/14, dort unter 5., http://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/.

[1299] EuGH, *Google Spain*, Rs. C-131/12, Rn. 36 ff., 98 = JZ 2014, 1009 (1016).

Die Anbieter sozialer Netzwerke sind, soweit sie personenbezogene Daten veröffentlichen, im Ausgangspunkt jedoch nicht mit den Betreibern von Suchmaschinen gleichzusetzen, sondern mit den unmittelbaren, primären Anbietern von Inhalten, also den Webseitenbetreibern, auf deren Seiten Suchmaschinenbetreiber verlinken. Betroffenen kommen insoweit – wie oben bereits besprochen – gegen die Anbieter sozialer Netzwerke und ggf. andere Nutzer ihre gesetzlichen Löschungsrechte zu, ohne dass die *Google*-Entscheidung des EuGH herangezogen werden muss.[1300]

Von erheblicher Bedeutung ist diese Entscheidung aber für ergänzende Funktionen in sozialen Netzwerken wie etwa Facebooks „Social Graph". Mit dieser Funktion – die aktuell in Deutschland noch gesperrt, in der US-amerikanischen Version aber bereits verfügbar ist[1301] – schafft Facebook eine Durchsuchbarkeit seines Netzwerks und wird damit selbst zu einer Art Suchmaschinenbetreiber. Die Funktion ermöglicht es, mit wenigen Schlagworten sowohl Personen nach bestimmten Kriterien auszuwählen, als auch eine gezielte Zusammenstellung von Inhalten angezeigt zu bekommen.[1302] So wäre es beispielsweise möglich, sowohl sehr alte Beiträge eines Nutzers eines sozialen Netzwerks als auch eine vollständige Übersicht all seiner Beiträge zu einem bestimmten Thema – gegebenenfalls aus dem Zusammenhang gerissen – mit wenigen Mausklicks angezeigt zu bekommen. Die *Google*-Entscheidung unterstreicht, dass eine solche Funktion gegenüber der ursprünglichen Veröffentlichung eine eigenständige, deutlich weitergehende Beeinträchtigung von Persönlichkeitsrechten bedeutet, da durch sie allen Nutzern die Möglichkeit gegeben wird, mehr oder weniger detaillierte Profile von Betroffenen zu erstellen.[1303] Sie stellt daher einen neuen Schritt der Datenverarbeitung dar, für den entsprechend entweder eine gesetzliche Ermächtigung oder eine Einwilligung vorliegen muss.[1304]

Hieraus folgt zum einen, dass die Einführung der Social-Graph Funktion in Deutschland bzw. der EU nur mit einer entsprechenden Einwilligung der Nutzer möglich wäre. Zum anderen lässt sich aber auch ein Recht der Betroffenen herleiten, gezielt auf die Zusammenstellung der

---

[1300] Vgl. auch *Dix*, in: Simitis, BDSG, § 35 Rn. 8, der allerdings die Verantwortlichkeit der Nutzer durch Anwendung des Haushaltsprivilegs beschränken will; zur Anbieter- und Nutzerverantwortlichkeit ausführlich oben unter D.I.3.

[1301] *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 25.

[1302] Vgl. *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 25.

[1303] EuGH, *Google Spain*, Rs. C-131/12, Rn. 37 f. = JZ 2014, 1009 (1011 f.); vgl. auch *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 25.

[1304] EuGH, *Google Spain*, Rs. C-131/12, Rn. 35, 41 = JZ 2014, 1009 (1011 f.); vgl. auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 96 f.

Ergebnisse der Suchfunktion Einfluss zu nehmen und ggf. eine Löschung zu verlangen. Auch hier erweist sich damit bereits das geltende Datenschutzrecht als in der Lage, mit sehr aktuellen Entwicklungen in sozialen Netzwerken umzugehen.

Zusammenfassend lässt sich daher sagen, dass wesentliche Elemente der Idee eines Rechts auf Vergessenwerden bereits im geltenden Recht verankert sind. Insbesondere in sozialen Netzwerken verschafft die umfassende Anbieterverantwortlichkeit auch für nutzergenerierte Inhaltsdaten[1305] den bestehenden Löschungsrechten dadurch Durchschlagskraft, dass Betroffene sich nicht darauf verweisen lassen müssen, eine Löschung von Inhaltsdaten bei dem jeweiligen anderen Nutzer zu beantragen. Er kann seinen Löschungsanspruch vielmehr direkt gegen den Anbieter des sozialen Netzwerks richten.

Dennoch bleibt das darüber hinausgehende Problem der Drittverbreitung bestehen, dass personenbezogene Daten aus dem sozialen Netzwerk heraus kopiert und dadurch weiter verbreitet werden können.[1306] Technische Lösungen wie ein automatisches „Ablaufdatum“ für personenbezogene Daten im Internet im Sinne einer Löschung sind zwar geeignet, gleichsam die Originale der Daten nach einem bestimmten Zeitraum zu entfernen.[1307] Sie erweisen sich aber als weitgehend wirkungslos gegenüber von Dritten erstellten Kopien. Insofern reduzieren Löschungsansprüche und automatische Löschungsmechanismen zwar in gewissem Umfang die verfügbaren Daten und leisten damit einen Beitrag zur Sicherung der informationellen Selbstbestimmung. Sie stellen aber keine abschließende Lösung dar, um nachhaltig und vollständig personenbezogene Spuren im Internet zu beseitigen und eine umfassende Informationskontrolle durch die Betroffenen zu gewährleisten.[1308]

[1305] Hierzu ausführlich oben unter D.I.3.a)aa).

[1306] *Kipker/Voskamp*, DuD 2012, 737 (741 f.) verneinen deshalb die Anwendbarkeit des Rechts auf Vergessenwerdens auf soziale Netzwerke, da dies insbesondere im Hinblick auf die verschärften Sanktionsmöglichkeiten des Art. 83 DS-GVO zu unüberschaubaren Haftungsrisiken für die Verantwortlichen im Falle eines Verstoßes führen würde. Diese Auffassung geht indes zu weit: Jedenfalls in dem Rahmen, in dem die Anbieter und sonstigen Verantwortlichen in sozialen Netzwerken einem Löschungsbegehren mit vertretbarem Aufwand nachkommen können, wäre es eine unverhältnismäßige Einschränkung der Betroffenenrechte, einen entsprechenden Anspruch grundsätzlich zu verneinen. Dies betrifft insbesondere die Pflicht, Dritte, an welche die Daten bewusst durch den Verantwortlichen weitergegeben wurden, über das Löschungsbegehren des Betroffenen zu informieren.

[1307] Hierzu *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107).

[1308] So auch bereits *Mayer-Schönberger*, Die Tugend des Vergessens, S. 213. *Hermstrüwer*, Informationelle Selbstgefährdung, S. 340 f. weist zudem darauf hin, dass der Status Quo Bias die Effektivität aktiv auszuübender Löschungsrechte erheblich untergraben könnte.

iii) Recht auf Datenportabilität

Es wurde bereits gezeigt, dass soziale Netzwerke zu einem natürlichen Monopol tendieren, da es für Nutzer interessanter ist, sich in einem Netzwerk anzumelden, in dem bereits viele ihrer Bekannten und andere Nutzer angemeldet sind.[1309] Diese Tendenz wird dadurch verstärkt, dass es für Nutzer einen erheblichen Aufwand bedeuten kann, ein einmal erstelltes Profil mitsamt seiner Kontakte in ein anderes soziales Netzwerk zu verlagern. Es bestehen damit erhebliche Lock-In Effekte[1310], die einen effektiven Wettbewerb unter Anbietern sozialer Netzwerke erschweren, wenn nicht gar verhindern.[1311]

Auf technischer Ebene könnte hier Abhilfe geschaffen werden, indem die Möglichkeit geboten wird, ein einmal erstelltes Profil mit wenig technischem Aufwand in ein anderes soziales Netzwerk zu übertragen – also insbesondere die hochgeladenen Fotos und zumindest die von einem Nutzer über sich selbst eingestellten Profilinformationen. Voraussetzung wäre eine Schaffung von miteinander kompatiblen Speicherungsformaten der Profile und die Möglichkeit, diese zu extrahieren.[1312] Rechtlich übersetzt bedeutet dies ein Recht auf Datenportabilität. Während ein solches im bisherigen Recht nicht festgeschrieben ist, war es bereits in allen drei Entwürfen der DS-GVO – freilich im Detail in unterschiedlicher Ausgestaltung – enthalten und ist nunmehr in Art. 20 DS-GVO normiert. Indem es auf die Reduzierung der Marktmacht und Lock-In Effekte einzelner Anbieter abzielt, bietet es eine Chance zur indirekten Stärkung des Datenschutzes.[1313]

Es ist allerdings fraglich, wie durchsetzungsstark dieses Recht sein wird. Art. 20 Abs. 4 DS-GVO sieht vor, dass dieses Recht die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf. Diese zunächst unscheinbar anmutende Einschränkung erhält im Lichte der Fassung des Ratsentwurfs eine hohe Brisanz, wonach insbesondere keine Urheberrechte

---

[1309] Oben unter D.III.2.b)cc).

[1310] Der ökonomische Effekt des Lock-In bezeichnet die Situation, dass die Kosten eines Anbieterwechsels den wirtschaftlichen Nutzen, der aus dem Wechsel gezogen werden kann, übersteigen. Der Kostenbegriff ist dabei weit zu verstehen: Es handelt sich mitnichten nur um direkte monetäre Kosten, sondern insbesondere auch die zu investierende Zeit und damit verbundene Opportunitätskosten. Vgl. hierzu instruktiv *Greve*, Staatliche Gewährleistungsverantwortung für offene Standards, S. 49 ff. , *Van Alsenoy u.a.*, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf, S. 25.

[1311] *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 142 f.; *Neuberger*, in: Neuberger/Gehrau (Hrsg.), Soziale Netzwerke, S. 46; *Pariser*, Filter Bubble, S. 40 f.; *Sandfuchs*, Privatheit wider Willen, S. 237.

[1312] *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 142; *Kipker/Voskamp*, DuD 2012, 737 (740); sehr ausführlich zur Begrifflichkeit einheitlicher technischer Standards *Greve*, Staatliche Gewährleistungsverantwortung für offene Standards, S. 59 ff.

[1313] Vgl. auch *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107); *Kühling/Martini*, EuZW 2016, 448 (450); *Schantz*, NJW 2016, 1841 (1845); *Dammann*, ZD 2016, 307 (308).

und sonstigen geistigen Eigentumsrechte verletzt werden sollten. Soziale Netzwerke könnten versuchen, einen Großteil der Profildaten unter diese Ausnahmeklausel zu fassen, mit dem Argument, das Profil in seiner Gesamtheit, insbesondere mit seinen Vernetzungen, sei vor allem den eigenen Algorithmen und Programmierungen geschuldet und müsse daher nicht herausgegeben werden.

Dieses Argument überzeugt indes jedenfalls für die unmittelbar vom Nutzer bereitgestellten Daten nicht. Zumindest die eigenhändig eingefügten Angaben sowie gegebenenfalls hochgeladene Fotos und Ähnliches – welche für die Selbstdarstellung sehr wichtig sein können – dürften daher in jedem Fall herauszugeben sein und dadurch den Wechsel in ein anderes Netzwerk erleichtern.

Allerdings ist der Nutzen eines Rechts auf Datenportabilität in sozialen Netzwerken in hohem Maße davon abhängig, dass auch eine Wechselbereitschaft der Freunde und Kontakte besteht, aufgrund derer sich ein grundsätzlich wechselwilliger Nutzer überhaupt in dem sozialen Netzwerk befindet. Um hier effektiv Lock-In-Effekte zu verhindern, müsste das Recht nicht nur Vorgaben zur Portabilität der Daten machen, sondern darüber hinaus eine Interoperabilität sowie eine diensteübergreifende Kommunikation verlangen.[1314] Konkret könnte dies so aussehen, dass die Möglichkeit geschaffen würde, das eigene Profil in ein datenschutzfreundliches soziales Netzwerk zu verlegen, über Interoperabilitätsvorgaben aber in Kontakt mit beispielsweise bei Facebook verbliebenen Kontakten zu bleiben.

Dies würde indes einen erheblichen Eingriff in die wirtschaftlichen Freiheiten der Anbieter der sozialen Netzwerke bedeuten: Sie müssten eine Infrastruktur zur Nutzung und Vernetzung bereitstellen, ohne mit jedem Nutzer einen Nutzungsvertrag zu haben und entsprechend von diesen eine Bezahlung in Form von Nutzungsgebühren oder Daten zu erhalten. Sie würden damit verpflichtet, ihre Konkurrenten erheblich zu unterstützen, ohne hierdurch einen eigenen wirtschaftlichen Nutzen zu haben. Konkret im Fall von Facebook könnten sich viele Nutzer entscheiden, „das Beste aus beiden Welten“ zu haben, nämlich einerseits ein datenschutzfreundliches, kostenloses, kleines Netzwerk für das eigene Profil, andererseits aber auch die enorme Reichweitenwirkung und Vernetzung durch Facebook. Man kann sich freilich auf den Standpunkt stellen, dass gerade diese Konsequenz einen sehr positiven Effekt auf den

[1314] Instruktiv zur Interoperabilität: *Greve*, Staatliche Gewährleistungsverantwortung für offene Standards, S. 49 ff., 169 ff.; *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 143; *Sandfuchs*, Privatheit wider Willen, S. 238; vgl. auch *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107); *Kipker/Voskamp*, DuD 2012, 737 (740).

Wettbewerb haben wird und es sich daher um eine sinnvolle Stärkung von Verbraucherrechten handeln würde.[1315] Zudem sind Interoperabilitätsvorgaben auch in anderen Regulierungsbereichen, etwa im Rahmen des Telekommunikationsmarktes, bekannt und legitimierbar.[1316]

Speziell im Fall von sozialen Netzwerken, bei welchen die Vernetzung der Nutzer untereinander und die Zahl der angemeldeten Profile gleichsam das zentrale „Betriebsvermögen" darstellt, dürfte sich eine solche Interoperabilitätsvorgabe von Nutzerprofilen indes als unverhältnismäßig erweisen. Letztendlich beruht dieses Ergebnis auf einer angemessenen Abwägung von Nutzer- und Anbieterinteressen: Ein Recht auf Datenportabilität ermöglicht es den Nutzern, ihre Profil selbstbestimmt und unter Vermeidung technischer Lock-In Effekte in eine anderes soziales Netzwerk zu verlegen. Es ist aber – ebenso wie im Rahmen des Kopplungsverbotes[1317] – nicht ersichtlich, warum das Recht ihn darüber hinaus vor einer Wechselunwilligkeit seiner Kontakte schützen sollte. Letztendlich hat es der einzelne Nutzer in der Hand, bei seinen Kontakten ebenfalls um einen Wechsel in ein anderes Netzwerk zu werben. Soweit dies nicht von Erfolg gekrönt ist, weil sich diese entweder aus aufrichtiger Trägheit oder einer anderen Interessengewichtung als wechselunwillig erweisen, stellt dies ein allgemeines Lebensrisiko dar, welches nicht vom Recht beseitigt werden muss.

cc) Verbandsklagerechte: Datenschutz als verbraucherschützende Vorschriften

Eine weitere Möglichkeit, den Selbstdatenschutz effektiver zu gestalten, ist die Ergänzung des Datenschutzrechts um Elemente des klassischen Verbraucherschutzrechts, insbesondere Verbandsklagerechte. Die bloße Normierung von Individualrechten und Regulierung von Datenverarbeitungsprozessen läuft leer, wenn aufgrund von Macht- und Informationsgefällen ein strukturelles Vollzugsdefizit besteht. Dies ist im Rahmen des Datenschutzrechts und

[1315] So *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 143.

[1316] *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 143; ausführlich hierzu *Greve*, Staatliche Gewährleistungsverantwortung für offene Standards, S. 215 ff. unter Verweis auf bestehende Interoperabilitätsvorgaben z.B. im Bereich von digitalen Fernsehempfangsgeräten und allgemein des elektronischen Kommunikationsnetzwerks zwischen Netzabschlusspunkten, sowie zwischen Netz und Endgeräten. Er verweist aber auch auf verbreitet fehlende Vorgaben im Bereich der Nachrichtencodierung und damit eine fehlende Interoperabilität von Endgeräten in zahlreichen Bereichen; unter Annahme einer staatlichen Privatisierungsfolgenverantwortung und hieraus resultierender Gewährleistungsverantwortung plädiert er für strengere Interoperabilitätsvorgaben auch auf der Ebene der Nachrichtencodierung.

[1317] Hierzu bereits oben unter D.III.2.b)cc).

speziell mit Blick auf soziale Netzwerke jedenfalls teilweise der Fall.[1318] Gerade bei großen sozialen Netzwerken wie Facebook ist es für den einzelnen Nutzer sehr schwierig, individuell seine Rechte durchzusetzen. Eine Beschwerde an die Datenschutzbehörden ist zwar stets möglich und auch zukünftig nach Art. 77 Abs. 1 DS-GVO vorgesehen, führt aber zu langwierigen Verwaltungsverfahren, die bisher häufig aufgrund von kollisionsrechtlichen Fragen scheiterten.[1319]

Tatsächlich hat die Bundeszentrale für Verbraucherschutz bereits wichtige Verfahren unter anderem gegen Facebook angestrengt, um die Datenverarbeitungspraktiken unter AGB-rechtlichen Aspekten gemäß § 1 Abs. 1 UKlaG kontrollieren zu lassen.[1320] Dies ist sehr zu begrüßen, nicht zuletzt wegen der sehr viel klareren kollisionsrechtlichen Lage aufgrund von Art. 6 Abs. 1 Rom-I VO, wonach das Marktortprinzip für den Verbraucher und damit völlig unstreitig deutsches Recht gilt.[1321]

Ob es sich bei datenschutzrechtlichen Vorschriften um verbraucherschützende Vorschriften im Sinne von § 2 Abs. 1 UKlaG handelt und somit ein Verbandsklagerecht über AGB-rechtliche Fragen hinaus besteht, war bisher umstritten.[1322] Insbesondere von der obergerichtlichen Rechtsprechung wurde ablehnend ins Feld geführt, das BDSG diene dem Schutz des allgemeinen Persönlichkeitsrechts, nicht speziell dem Schutz von Verbrauchern.[1323] Dies war indes bereits in der zivilrechtlichen Argumentation fragwürdig, da beispielsweise auch § 439 BGB als verbraucherschützend anerkannt ist, obwohl er für alle Käufer und nicht nur für Verbraucher gilt.[1324] Jedenfalls verkannte diese Ansicht aber die Bedeutung des

---

[1318] Vgl. *Sandfuchs*, Privatheit wider Willen, S. 237 ff.; *Roßnagel/Richter/Nebel*, ZD 2013, 103 (106); *Spiecker gen. Döhmann*, K&R 2012, 717 (723); vgl. allgemein zu Vollzugsdefiziten im Datenschutzrecht: *Klar*, DÖV 2013, 103 (108 f.); *Weidlich-Flatten*, ZRP 2014, 196 (196); *Kühling/Sivridis/Schwuchow/Burghardt*, DuD 2009, 335 (336 ff.).

[1319] *Spindler*, ZD 2016, 114 (115); vgl. auch OVG Schleswig, ZD 2013, 364 (366); VG Schleswig, ZD 2013, 245 (245 f.); VG Hamburg, ZD 2016, 243 (244 ff.); vgl. hierzu bereits oben unter C.II. Insoweit wird die DS-GVO eine Verbesserung darstellen, indem einerseits ein einheitliches Datenschutzrecht gilt und Nutzern andererseits zumindest das Recht garantiert wird, vor ihrer eigenen nationalen Aufsichtsbehörden Beschwerde einzulegen, vgl. Art. 77 Abs. 1 DS-GVO. Aktuell sind hierfür häufig noch die Aufsichtsbehörden im Sitzland des Datenverarbeiters zuständig. Vgl. ausführlich zu Zuständigkeiten der Aufsichtsbehörden nach der DS-GVO *Ngyuen*, ZD 2015, 265 (266 ff.).

[1320] KG Berlin, ZD 2014, 412 (413 ff.); LG Berlin, ZD 2015, 133 (134 ff.); vgl. auch LG Berlin, ZD 2013, 451 (452 f.); LG Berlin, ZD 2012, 276 (277 f.).

[1321] Instruktiv: *Weller/Nordmeier*, in: Spindler/Schuster, Art. 6 Rom-I-VO, Rn. 11 ff.

[1322] Befürwortend: *Micklitz*, in: MüKo-ZPO, Bd. 3, § 2 UKlaG Rn. 40 m.w.N.; *Spindler*, ZD 2016, 114 (115); *Köpernik*, VuR 2014, 240 (242); ablehnend: OLG Frankfurt, GRUR 2005, 785 (786) m.w.N.; OLG Düsseldorf, ZUM-RD 2004, 236 (237); *Köhler*, in: Ders./Bornkamm, UWG, § 2 UKlaG Rn. 13; *Schulz*, ZD 2014, 510 (512 ff.); *Sandfuchs*, Privatheit wider Willen, S. 245.

[1323] OLG Frankfurt, GRUR 2005, 785 (786) m.w.N.; OLG Düsseldorf, ZUM-RD 2004, 236 (237); so auch *Schulz*, ZD 2014, 510 (512); *Sandfuchs*, Privatheit wider Willen, S. 245.

[1324] *Micklitz*, in: MüKo-ZPO, Bd. 3, § 2 UKlaG Rn. 40.

Datenschutzrechts und die möglichen benachteiligenden Konsequenzen einer rechtswidrigen Datenverarbeitung für Verbraucher in einer zunehmend digitalen Ökonomie. Auch wurde bereits von mehreren Obergerichten anerkannt, dass Verstöße gegen Datenschutzvorschriften gemäß § 4 Nr. 11 UWG unlauter sein können, was unter Wettbewerbern zunehmend zu erfolgreichen Abmahnungen bzw. Untersagungen führte.[1325]

Mit der am 17. Februar 2016 verabschiedeten Neufassung des § 2 Abs. 2 S. 1 Nr. 11 UKlaG[1326] hat der Gesetzgeber nunmehr klargestellt, dass Vorschriften über die Erhebung oder Zulässigkeit der Verarbeitung personenbezogener Daten zu kommerziellen Zwecken, insbesondere der Werbung oder Profilbildung, im Verhältnis von Verbrauchern und Unternehmern verbraucherschützende Qualität zukommt.[1327] Zudem wurde der Unterlassungsanspruch um einen Beseitigungsanspruch ergänzt, um eine noch effektivere Durchsetzung der Verbraucherschutznormen zu gewährleisten.[1328] Verbraucherschutzverbände und andere Anspruchsberechtigte gemäß § 3 Abs. 1 Nr. 1 UKlaG können somit nunmehr gegen Unternehmer vorgehen, die auf andere Weise als aufgrund der Verwendung von allgemeinen Geschäftsbedingungen gegen Datenerhebungs- und -verarbeitungsvorschriften verstoßen. Die hieraus resultierende Stärkung von Betroffenen- und Verbraucherrechten ist sehr zu begrüßen und stellt sowohl eine sinnvolle als auch eine notwendige Reaktion auf die stark gestiegenen Möglichkeiten unternehmerischer Datenverarbeitung dar.[1329] Die Gesetzesänderung ist auch mit der DS-GVO vereinbar, welche in Art. 80 Abs. 2 die Mitgliedstaaten ermächtigt, ein entsprechendes Verbandsklagerecht zu erlassen.[1330]

b) „Risk-Based Approach“

Anders als Maßnahmen des Selbstdatenschutzes versucht der risikobasierte Ansatz (Risk-Based Approach) die Komplexität von Datenschutzvorgaben dadurch zu verringern, dass die Pflichten der Datenverarbeiter in Relation zu dem Risiko für die Nutzer gesetzt werden.

[1325] OLG Köln, ZD 2014, 421 (421) m.w.N.; OLG Stuttgart, MMR 2007, 437 (437 f.); OLG Hamburg, ZD 2013, 511 (512); vgl. auch LG Berlin, ZD 2015, 133 (134 f.); *Buchner*, Facebook zwischen BDSG und UWG, in: FS Köhler, S. 58 ff.; *Micklitz*, in: MüKo-ZPO, Bd. 3, § 2 UKlaG Rn. 40; BT-Drs. 18/4631, S. 20; *Köpernik*, VuR 2014, 240 (241 f.); ablehnend *Sandfuchs*, Privatheit wider Willen, S. 245.

[1326] Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts, BGBl. I 2016, S. 233 ff.

[1327] Kritisch hinsichtlich der engen Begrenzung *Spindler*, ZD 2016, 114 (116).

[1328] BT-Drs. 18/4631, S. 8, 20.

[1329] BT-Drs. 18/4631, S. 22; *Spindler*, ZD 2016, 114 (119); vgl. auch *Micklitz*, in: MüKo-ZPO, Bd. 3, § 2 UKlaG Rn. 40; Art. 29 DatSchGruppe, Stellungnahme WP 227, S. 3; *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 130; *Weidlich-Flatten*, ZRP 2014, 196 (198); *Sandfuchs*, Privatheit wider Willen, S. 244 ff.; vgl. auch *Spiecker gen. Döhmann*, K&R 2012, 717 (723 f.); a.A. *Schulz*, ZD 2014, 510 (512 ff.).

[1330] Vgl. auch *Spindler*, ZD 2016, 114 (119).

Benachrichtigungspflichten gegenüber Aufsichtsbehörden, aber auch spezielle Voraussetzungen für die Aufbewahrung und Speicherung sollen nicht der bloßen Form halber anwendbar sein, sondern nur in dem Umfang, der dem mit der Datenverarbeitung verbundenen Risiko angemessen ist.[1331] Dieser Ansatz ist nicht grundsätzlich neu, sondern findet sich als Skalierung der Compliancepflichten von Datenverarbeitern unter anderem bereits in Art. 17 Abs. 1 S. 2 und 20 Abs. 1 DSRL. Auch die Hervorhebung besonders schutzwürdiger Arten von Daten in Art. 8 DSRL bzw. § 3 Abs. 9 BDSG kann als Teil eines risikobasierten Ansatzes gesehen werden.[1332] Zudem bestehen offensichtliche Parallelen zu dem stets zu beachtenden Verhältnismäßigkeitsprinzip.

Seit dem Beginn der Verhandlungen über die DS-GVO erhält der risikobasierte Ansatz allerdings eine vermehrte Aufmerksamkeit. In den Entwürfen der Kommission, des Parlaments und des Rates wird – in einer rein textbasierten Analyse – das Wort „Risiko" mit jedem Entwurf häufiger verwendet.[1333] Auch in der endgültigen Fassung kommt dem Konzept des Risikos eine prominente Stellung zu.

Gemäß Artikel 24 DS-GVO ist bereits der Maßstab für die pflichtgemäße Einhaltung der Vorschriften der DS-GVO durch den für die Datenverarbeitung Verantwortlichen anhand einer Risikoabwägung zu bestimmen. Bestimmte Sicherheitspflichten (Art. 32 DS-GVO) sowie die Implementierung technischer und organisatorischer Maßnahmen zum Datenschutz (Art. 25 DS-GVO) werden ebenfalls einer Risikoabwägung unterstellt. Benachrichtigungspflichten gegenüber den Aufsichtsbehörden und dem Betroffenen im Falle von Datenlecks („data breaches") bestehen zudem gemäß Art. 33, 34 DS-GVO nur, wenn infolge dieses Lecks ein (hohes) Risiko für die Rechte und Freiheiten natürlicher Personen besteht.[1334] Wann eine Risikoabwägung im Sinne einer Datenschutzfolgenabschätzung *vor* der Vornahme der Datenverarbeitung angezeigt ist, spezifiziert Art. 35 DS-GVO. Der Fokus der Regulierung bewegt sich dabei generell fort von der bloßen Erhebung von Daten und hin zu der konkreten Verwendung von Daten; insbesondere pseudonym genutzte Daten werden schwächeren

[1331] Art. 29 DatSchGruppe, Stellungnahme WP 218, S. 2; *Zimmermann*, Einwilligung im Internet, S. 52; *Thoma*, ZD 2013, 578 (580 f.); vgl. auch *Rogall-Grothe*, ZRP 2012, 193 (195); instruktiv auch *Marschall*, in: Roßnagel (Hrsg.), Europäische DS-GVO, § 3 Rn. 159 ff.

[1332] Art. 29 DatSchGruppe, Stellungnahme WP 218, S. 2; *Thoma*, ZD 2013, 578 (580); vgl. auch *Gierschmann*, ZD 2016, 51 (53).

[1333] Ausführlich: *Veil*, ZD 2015, 347 (348); vgl. auch bereits *Thoma*, ZD 2013, 578 (580 f.).

[1334] Vgl. auch *Veil*, ZD 347 (348); *Gierschmann*, ZD 2016, 51 (53) weist allerdings zutreffend darauf hin, dass vergleichbare Risikoabwägungen auch bisher nach § 42a BDSG getroffen werden mussten, indem Meldepflichten nur bei der Verletzung von besonders sensitiven Daten galten, sofern schwerwiegende Beeinträchtigungen von Betroffenen drohten.

Regelungen unterworfen, beispielsweise in Form einer gelockerten Zweckbindung gemäß Art. 6 Abs. 4 lit. e) DS-GVO.[1335]

Der risikobasierte Ansatz ist zu begrüßen, soweit er eine effektivere Umsetzung der Datenschutzvorschriften befördert: Wo Datenschutz nur um der bloßen Form willen betrieben wird, leidet nicht zuletzt seine Akzeptanz. Es ist insofern konsequent, dass der Umfang datenschutzrechtlicher Pflichten in Relation zu den tatsächlich vorgenommenen Datenverarbeitungen stehen sollte. In eben dieser Hinsicht handelt es sich bei dem risikobasierten Ansatz auch um ein seit langem in das geltende Datenschutzrecht integriertes Konzept.[1336]

Sehr kritisch ist dieser Ansatz indes dort zu beurteilen, wo er dazu dient, wirtschaftliche Interessen an einfacherer Datenverarbeitung zu fördern und damit Rechte von Betroffenen bei einem vermeintlich niedrigen Risiko zu verringern. Dies kann es insbesondere im Zusammenhang mit gelockerten Vorgaben zur Zweckbindung und -änderung im Rahmen von Big Data Anwendungen der Fall sein. Wenn der risikobasierte Ansatz als „eine der wenigen echten Modernisierungen“ gelobt wird, „die die Datenschutzreform bringen könnte“[1337], so bezieht sich dies vor allem auf derartige implizite Beschneidungen von Betroffenenrechten.[1338] Es ist unbestreitbar, dass die Grundsätze der Zweckbindung und der Datensparsamkeit einer uneingeschränkten Nutzung zu Big Data Zwecken entgegensteht, ist doch bei Big Data und dem damit verbundenen Data Mining in aller Regel am Anfang unklar, welche Erkenntnisse sich am Ende aus einem Datensatz ziehen lassen.[1339]

Gerade dies zeigt aber auch, warum ein derart verstandener risikobasierter Ansatz ein erhebliches Problem für die informationelle Selbstbestimmung Betroffener darstellt: Da zu Beginn einer solchen Datenverarbeitung unklar ist, welche Ergebnisse aus ihr folgen können, ist auch die vorausgehende Datenschutzfolgenabwägung und eine Einteilung in „normale“ und

---

[1335] Art. 29 DatSchGruppe, Stellungnahme WP 218, S. 2; vgl. auch Erwägungsgrund 28 DS-GVO, wonach Maßnahmen der Pseudonymisierung „die Verantwortlichen und Auftragsdatenverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen“ kann.

[1336] Art. 29 DatSchGruppe, Stellungnahme WP 218, S. 2.

[1337] *Veil*, ZD 2015, 347 (348).

[1338] Vgl. Art. 29 DatSchGruppe, Stellungnahme WP 218, S. f.

[1339] *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 14 f.; *Martini*, DVBl. 1481 (1484); *Weichert*, ZD 2013, 251 (252, 256 f.); *Hill*, DÖV 2014, 213 (215); vgl. auch *Fehling*, Privacy, in: ders. u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 143 f. – *Erscheinen in Vorbereitung*.

„besonders risikobehaftete Datenverarbeitung“[1340] nicht möglich. Es gilt vielmehr auch hier die vom Bundesverfassungsgericht geäußerte Feststellung, dass es „kein belangloses Datum“ mehr gibt[1341] und entsprechend erst recht keine belanglose Verarbeitung und Verknüpfung mit weiteren Daten zu *ex ante* unbekannten Ergebnissen.[1342] Denn die Bedeutung einer Datenverarbeitung für das allgemeine Persönlichkeitsrecht lässt sich nur im konkreten Verarbeitungszusammenhang beurteilen, welcher wiederum von den verfolgten Zwecken bestimmt wird.[1343]

Natürlich ist an dieser Stelle eine Abwägung zu treffen: Dem Verlust an Rechten Betroffener steht ein möglicher Effizienzgewinn in der Datenverarbeitung und damit mögliche ökonomische Vorteile von Big Data Anwendern, aber auch den Betroffenen selbst gegenüber. In den USA sind es gerade solche Vorteile, die als Argument gegen einen umfassenden Datenschutz ins Feld geführt werden: Ein ungehinderter Informationsfluss wird als Förderung, gar Voraussetzung für ökonomische Transaktionen und das Finden informierter Entscheidungen gesehen.[1344] *Strahilevitz* – als einer der bekanntesten Theoretiker in der US-amerikanischen *Privacy*-Forschung – stellt zudem die These auf, dass nur eine weitgehende Transparenz von persönlichen Daten rassistische Vorurteile und Diskriminierung reduzieren könnte, indem Individuen basierend auf ihren konkreten Daten und nicht auf stereotypen Zuschreibungen beurteilt werden.[1345] Datenschutz sei daher nur dort gerechtfertigt, wo konkrete Schäden einer Veröffentlichung ausgeschlossen werden müssten.

Diese effizienzorientierte Risikobetrachtung, die nur bereits eingetretene Schäden beseitigen will, verkennt aber die grundlegende Bedeutung, die die informationelle Selbstbestimmung für

---

[1340] So *Veil*, ZD 2015, 347 (348); in eine ähnliche Richtung argumentieren auch *Schneider/Härting*, ZD 2011, 63 (65), indem sie eine Aufhebung des Verbots mit Erlaubnisvorbehalt für alle nicht-sensiblen Datenverarbeitungen fordern. *Thoma*, ZD 2013, 578 (578 ff.) begrüßt zwar den Risk-Based Approach, lässt aber ausdrücklich offen, „welche Arten oder Typen von Datenverarbeitung als besondere risikoreich zu klassifizieren sind“ und weist darauf hin, dass dies je nach Rechtstradition in den europäischen Mitgliedstaaten sehr unterschiedlich gehandhabt werden könnte, woraus ein mögliches Problem in der Rechtsvereinheitlichung resultiere (a.a.O., S. 578 f.).

[1341] BVerfGE 65, 1 (45) – Volkszählung; *Taeger/Schmidt*, in: Taeger/Gabel, Einf BDSG, Rn. 44.

[1342] *Martini*, DVBl. 2014, 1481 (1484) vgl. auch *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 102 f.; *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner, S. 435.

[1343] *Taeger/Schmidt*, in: Taeger/Gabel, Einf BDSG, Rn. 44; *Simitis*, in: Simitis, BDSG, § 1 Rn. 66, § 3 Rn. 251; *Nebel*, Facebook knows your vote!, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 102 f.; vgl. auch *Weichert*, ZD 2013, 251 (255).

[1344] Vgl. *Strahilevitz*, 126 Harv. L. Rev. 2010 (2022 ff.) 2012-2013 m.w.N., welcher ausführlich analysiert, welche Personengruppen von Big Data gewinnen und verlieren können und das Fazit zieht, dass zu viel *Privacy* ebenso schädlich sein könne wie zu wenig, a.a.O., S. 2039 f.; ausführlich aus rechtsvergleichender Perspektive auch *Fehling*, Privacy, in: ders. u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 140 ff. – *Erscheinen in Vorbereitung*; *Sandfuchs*, Privatheit wider Willen, S. 94 ff.

[1345] *Strahilevitz*, 126 Harv. L. Rev. 2010 (2018 ff.) 2012-2013.

die Ausformung der eigenen Persönlichkeit und letztlich für die Konstitution eines demokratischen Gemeinwesens hat.[1346] Kurzfristigen ökonomischen Effizienzgewinnen stehen kaum abschätzbare Risiken für die langfristige informationelle Selbstbestimmung gegenüber. Der europäische Ansatz, Datenschutz als Risikovorsorgerecht zu begreifen und einen umfassenden Vorfeldschutz für personenbezogene Daten zu gewährleisten,[1347] erweist sich hier als deutlich angemessener, um diesen Gefahren zu begegnen.

Es ist daher zwar grundsätzlich zu begrüßen, den konkreten Umfang der Pflichten von Datenverarbeitern in der Verhältnismäßigkeitsabwägung in eine Relation zu dem mit der Datenverarbeitung verbundenen Risiko zu setzen.[1348] Das tatbestandsmäßige Bestehen von Pflichten – und damit korrespondierend von Betroffenenrechten – von einer kaum seriös vorzunehmenden Datenschutzfolgenabwägung abhängig zu machen, verletzt indes in nicht zu rechtfertigender Weise die in Artikel 8 und 9 GRCh normierten bzw. aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleiteten Betroffenenrechte auf Privatheit und informationelle Selbstbestimmung und damit auch das allgemeine Persönlichkeitsrecht.[1349]

Soweit der risikobasierte Ansatz also auf eine tatbestandsmäßige Einschränkung von Betroffenenrechten abzielt und nicht nur auf eine verhältnismäßige Anpassung der Pflichten der Datenverarbeiter, verschärft er bestehende datenschutzrechtliche Probleme. Insbesondere Durchsetzungsdefizite von Betroffenenrechten infolge mangelnder Transparenz und Überforderung bei der Einwilligung werden keinesfalls behoben. Es wirkt vielmehr so, als ob auf das Fehlen effektiver Durchsetzungsmechanismen mit der Abschaffung der in ihrer Durchsetzung problematischen Rechte geantwortet werden soll.

Dies gilt auch und speziell für soziale Netzwerke, in denen teilweise sehr persönliche Daten gespeichert sind. Tatsächlich ist angesichts der potentiellen Sensibilität dieser Daten –

[1346] Ausführlich zu dieser Bedeutung *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 569 ff. m.w.N.; *Albers*¸ Informationelle Selbstbestimmung, S. 454 ff.; *Fehling*, Privacy, in: ders. u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 140 ff. – *Erscheinen in Vorbereitung*; BVerfGE 65, 1 (42 f.) – Volkszählung.

[1347] Instruktiv und rechtsvergleichend zu den USA *Fehling*, Privacy, in: ders. u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 137 ff. – *Erscheinen in Vorbereitung*; vgl. auch *Strahilevitz*, 126 Harv. L. Rev. 2010 (2035 f.) 2012-2013; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 39 ff., 138. Ausführlich zur Kontextbezogenheit des Informationsgehalts, der sich aus Daten gewinnen lässt, auch *Albers*¸ Informationelle Selbstbestimmung, S. 87 ff.

[1348] *Veil*, ZD 2015, 347 (348 ff.); *Thoma*, ZD 2013, 587 (578 f.); vgl. auch *Rogall-Grothe*, ZRP 2012, 193 (195).

[1349] Art. 29 DatSchGruppe, Stellungnahme WP 218, S. 3; teilweise a.A. *Zimmermann*, Einwilligung im Internet, S. 53 für Konstellationen, in denen aktuell die Wirksamkeit und Geeignetheit einer Einwilligung sehr fragwürdig sind: Wenn aktuell schon keine selbstbestimmte Entscheidungsmöglichkeit vorliege, könne eine Beschränkung der Einwilligungsvoraussetzungen auch keine weitergehende Beschränkung der Selbstbestimmung bedeuten.

beispielsweise im Falle von Angaben oder möglichen Rückschlüssen zur religiösen oder politischen Überzeugung oder zur sexuellen Orientierung – ohnehin fraglich, inwieweit der „moderne“ risikobasierte Ansatz überhaupt sinnvoll auf diese anzuwenden ist. Angesichts der schieren Menge von Daten und deren teilweise erheblicher Sensibilität müsste regelmäßig von einer besonders risikobehafteten Datenverarbeitung ausgegangen werden – selbst im Falle von *prima facie* irrelevanten Formen der Datenverarbeitung.[1350] In diesem Fall käme es aber zu keiner der gewünschten und beabsichtigten Vereinfachungen.

Der in den aktuellen Entwürfen zur DS-GVO zum Ausdruck kommende moderne risikobasierte Ansatz stellt daher im Ergebnis keine Lösung für die in sozialen Netzwerken bestehenden datenschutzrechtlichen und regulatorischen Probleme dar.

4. Freiheitbeschränkung zum Freiheitsschutz: Paternalistische Ansätze

Über die soeben skizzierten Maßnahmen zur Förderung des Selbstschutzes der Nutzer in sozialen Netzwerken hinaus kann zudem überlegt werden, ob zum Schutz der informationellen Selbstbestimmung ein paternalistischer „Schutz der Nutzer vor sich selbst“ geboten sein kann. Dieser bedeutet naturgemäß eine Freiheitseinschränkung, welche aber in engen Grenzen gerechtfertigt sein kann, wenn hierdurch beispielsweise erhebliche Rationalitätsdefizite im menschlichen Entscheidungsverhalten ausgeglichen und damit in langfristiger Hinsicht verfassungsrechtliche Freiheiten gesichert werden können.[1351] Zudem folgt aus der objektiven

[1350] Auch hier zeigt sich die praktische Unschärfe des risikobasierten Ansatzes: Freilich wäre eine Verwendung ausschließlich zu Werbezwecken *prima facie* vielleicht harmlos und nicht sonderlich risikobehaftet. Diese Verwendung zu Werbezwecken setzt aber die Generierung von Daten und Informationen voraus, die in anderem Kontext sehr sensibel sein könnten. Anekdotenhaft sei auf ein das Unternehmen Target verwiesen, das aus dem Kaufverhalten junger Frauen in Drogerien mittels Big Data Analysen Vorhersagen über Schwangerschaftsstadien treffen konnte, vgl. *Strahilevitz*, 126 Harv. L. Rev. 2010 (2022 f.) 2012-2013. Eine Regelung, die die Verwendung von Daten zu zunächst harmlosen Zwecken ohne weitere Voraussetzungen gestattet, kann damit zu einem erheblichen Kontrollverlust der Betroffenen über deutlich persönlichere Daten und Informationen führen.

[1351] Instruktiv: *Eidenmüller*, JZ 2011, 814 (815) m.w.N.; *Sandfuchs*, Privatheit wider Willen, S.116 ff., 155 ff.; vgl. auch *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 591 f.

Werteordnung des Grundgesetzes unter bestimmten Voraussetzungen die Zulässigkeit eines Wertepaternalismus.[1352]

Weder das aktuelle noch das zukünftige Datenschutzrecht der DS-GVO sehen derartige Maßnahmen zum Schutz der Nutzer vor sich selbst vor, sondern schützen nur vor Beeinträchtigungen durch Dritte sowie den Datenverarbeiter.[1353] Auch das Bundesverfassungsgericht betont grundsätzlich, dass es dem Einzelnen „regelmäßig möglich und zumutbar [ist], geeignete Vorsorgemaßnahmen zu treffen, um seine Geheimhaltungsinteressen zu wahren."[1354] Wie oben bereits dargelegt wurde, können soziale Netzwerke aber Gefahren für die informationelle Selbstbestimmung bedeuten, die für den Einzelnen nicht immer offensichtlich sind und die mitunter auch systematisch unterschätzt werden.[1355] Die Probleme in sozialen Netzwerken nur durch einen Appell an die Eigenverantwortung der Nutzer zu lösen, erscheint daher keinesfalls als umfassende Lösung.[1356] Es ist Teil der staatlichen Schutzpflicht, die Möglichkeit zur selbstbestimmten Kommunikationsteilhabe zu gewährleisten, um die Selbstschutzoption nicht zu einer bloßen Fiktion verkommen zu lassen.[1357] Entsprechend ist es nur konsequent, im Zusammenhang mit sozialen Netzwerken über paternalistische Maßnahmen nachzudenken.[1358]

[1352] *Eidenmüller*, JZ 2011, 814 (815); BVerfGE 7, 198 (205) m.w.N. – Lüth. Das GG stellt nach der vorstehend zitierten Rechtsprechung keine wertneutrale Ordnung auf, sondern errichtet ein Wertesystem, das den Schutz der „sich frei entfaltenden menschlichen Persönlichkeit und ihrer Würde" „innerhalb der sozialen Gemeinschaft" zu seinem Mittelpunkt erklärt. Diesen Grundsätzen darf keine rechtliche Regelung entgegenstehen. Die Verpflichtung des Staates zur Aufrechterhaltung dieser Werte kann unter bestimmten Voraussetzungen den Erlass von freiheitsbeschränkenden Regelungen oder das Treffen von freiheitsbeschränkenden Maßnahmen legitimieren. Derartigen Regelungen oder Maßnahmen käme dann ein wertepaternalistischer Charakter zu. In gleicher Weise stellt es beispielsweise eine Form des Wertepaternalismus dar, sittenwidrige Verträge als nichtig zu betrachten, vgl. *Eidenmüller*, a.a.O.

[1353] *Piltz*, Soziale Netzwerke, S. 59; *Spindler/Nink*, in: Spindler/Schuster, § 11 TMG, Rn. 3; vgl. auch *Sandfuchs*, Privatheit wider Willen, S. 133 f.

[1354] BVerfGK 9, 353 (358), Rn. 31 – Schweigepflichtentbindung; vgl. auch *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 587; dies betont auch *Buchholtz*, AöR 2015, 121 (135 ff.).

[1355] Hierzu bereits oben unter B.II..; vgl. auch *Grimmelmann*, 94 Iowa L.Rev. 1137 (1160 ff.), 2008-2009; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 240 ff.; allgemein zu Rationalitätsdefiziten im menschlichen Entscheidungsverhalten: *Thaler/Sunstein*, Nudge, S. 31 ff.; *Eidenmüller*, JZ 2011, 814 (815) m.w.N.

[1356] *Roßnagel*, Persönlichkeitsentfaltung, in: Bieber/Eifert (u.a.) (Hrsg.), Soziale Netze in der digitalen Welt, S. 277 f.; *Buchholtz*, AöR 2015, 121 (135 ff.); vgl. auch *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 592; *Hoffmann-Riem*, AöR 1998, 513 (532); *Fehling*, Evolving Law and Economics of Internet Privacy, in: Eger u.a. (Hrsg.), Economic Analysis of International Law, S. 105 f.; *Buchholtz*, AöR 2015, 121 (136); *Greve*, Drittwirkung, in: FS Kloepfer, S. 673.

[1357] BVerfGE 120, 274 (306), Rn. 180 – Onlinedurchsuchung; BVerfGK 9, 353 (358 f.) – Schweigepflichtentbindung; *Bäcker*, Der Staat (51) 2012, 91 (99 ff.); *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 587 f.; *Hoffmann-Riem*, AöR 1998, 513 (523, 527, 532).

[1358] So auch *Spindler/Nink*, in: Spindler/Schuster, § 11 TMG, Rn. 3; *Greve*, Drittwirkung, in: FS Kloepfer, S. 673; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 363 ff.

Hierbei können sowohl verhaltenssteuernde Maßnahmen im Sinne eines liberalen bzw. libertären Paternalismus[1359], als auch klassische Regulierungsmaßnahmen wie Zugangsbeschränkungen oder ausdrückliche Verbote bestimmter Handlungen in Betracht gezogen werden. Bevor aber beispielshafte, schematische Ansätze dargestellt werden, muss zunächst die Vielschichtigkeit der informationellen Selbstbestimmung in den Blick genommen werden, welche paternalistische Regelungen erschwert.

a) Informationelle Selbstbestimmung in sozialen Netzwerken als vielschichtiges Grundrecht

Informationelle Selbstbestimmung sowie die Art. 7 und 8 GrCH normierten Rechte auf Achtung des Privatlebens und des Schutzes der personenbezogenen Daten werden oft primär als Recht auf Geheimhaltung verstanden, mithin als Recht, andere von der unkontrollierten Kenntnisnahme persönlicher Informationen auszuschließen, freilich innerhalb gewisser Schranken.[1360] Ausgangspunkt ist hierbei die Formulierung des Bundesverfassungsgerichts, dass jeder befugt ist, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[1361] Anders als beispielsweise in den USA, in denen wie bereits ausgeführt eine stärker ökonomisierte Betrachtung von Daten vorherrscht und Datenschutz vor allem als Abwehrrecht gegen den Staat verstanden wird, kommt der informationellen Selbstbestimmung in Deutschland und Europa eine funktionelle Sicherungsfunktion für die individuelle Freiheitsausübung zu.[1362]

Nicht vergessen werden darf aber der spiegelbildliche kommunikative Aspekt informationeller Selbstbestimmung, Informationen bewusst preiszugeben und ihren Geheimhaltungsstatus

[1359] Instruktiv: *Thaler/Sunstein*, Nudge, S. 14 ff.; kritisch: *Wolff*, RW 2015, 194 (209 ff.); *Eidenmüller*, JZ 2011, 814 (817 ff.); *Hermstrüwer*, Informationelle Selbstgefährdung, S. 359 ff.

[1360] Beispielsweise betont von *Nietsch*, Anonymität, S. 38 ff.; vgl. zu den Schranken schon BVerfGE 65, 1 (43 f.) – Volkszählung; *Schmidt*, in: Taeger/Gabel, Einf BDSG, Rn. 16; ablehnend zu einem Missverstehen als eigentumsanaloger Verfügungsbefugnis *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 562 ff.; *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 40; instruktiv zu den Art. 7 und 8 GrCh und ihren Gemeinsamkeiten mit der informationellen Selbstbestimmung *Augsberg*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 7 Rn. 5, Art. 8 Rn. 6 GrCH; vgl. auch ausführlich *Eichenhofer*, Der Staat (55) 2016, 41 (55 ff.).

[1361] BVerfGE 65, 1, 43 – Volkszählung.

[1362] Hierzu ausführlich rechtsvergleichend *Sandfuchs*, Privatheit wider Willen, S. 94 ff.; *Fehling*, Privacy, in: ders. u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 125 ff. – *Erscheinen in Vorbereitung*; *Geminn/Roßnagel*, JZ 2015, 703 (704); *Mayer-Schönberger*, Die Tugend des Vergessens, S. 162 ff.; *ders.*, Informationsrecht als Gestaltungsaufgabe, in: FS Druey (Schweizer u.a., Hrsg.), S. 861 ff.; vgl. auch *Whitman*, Yale Law Journal (113) 2004, S. 1151 (1210 ff.).

anderen gegenüber gleichsam aufzuheben.[1363] Nur im Zusammenspiel dieser beiden Aspekte kann eine selbstbestimmte Entfaltung und Entwicklung der Persönlichkeit gelingen.[1364] Eine paternalistische Einschränkung der Nutzungs- oder Datenverarbeitungsmöglichkeiten in sozialen Netzwerken bewegt sich daher stets in einem Spannungsverhältnis von sowohl Schutz als auch Beschneidung der informationellen Selbstbestimmung.[1365]

Die Schaffung eines eigenen Persönlichkeitsbildes beruht immer auch auf der Konstruktion von Fremdbildern, die Personen mehr oder weniger bewusst vornehmen. Menschen präsentieren sich in unterschiedlichen Situationen auf verschiedene Weise und prägen damit das Bild, das ihr Gegenüber von ihnen bekommt, maßgeblich mit.[1366] Soziale Netzwerke übernehmen insoweit eine wichtige soziale Funktion, als sie es Nutzern ermöglichen, ein digitales Selbst von sich zu erschaffen.[1367] Mit diesem interagieren sie zunächst online mit anderen Nutzern. Es wirkt aber auch zurück in die analoge Welt: Das geschaffene digitale Selbst beeinflusst zum einen die analoge Fremdwahrnehmung, indem die Selbstdarstellung zusammen mit der Kommunikation und Interaktion Beziehungen prägt und weiterentwickelt. Zum anderen kann durch Feedback auf die Selbstdarstellung auch das eigene Selbstbild nachhaltig verändert werden.[1368] Eine Beschränkung der Möglichkeiten, sich in sozialen Netzwerken selbst zu präsentieren, stellt somit immer auch eine Beschränkung darin dar, seine Identität in der Beziehung zu anderen zu formen.

Es ist allgemein anerkannt, dass das Recht auf informationelle Selbstbestimmung im Allgemeininteresse eingeschränkt werden kann. Schon das Bundesverfassungsgericht hat im

---

[1363] Instruktiv: *Sandfuchs*, Privatheit wider Willen, S. 7 ff., 156 ff.; *Kutscha*, GR-Schutz im Inet, S. 47; *Greve*, Drittwirkung, in: FS Kloepfer, S. 672 f.; *Fehling*, Privacy, in: ders. u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 129 ff. – *Erscheinen in Vorbereitung*; *Masing*, NJW 2012, 2305 (2308); *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.) Offene Rechtswissenschaft, S. 587 f.; *Hoffmann-Riem*, AöR 1998, 513 (520 ff.); vgl. auch *Spindler*, GRUR-Beilage 2014, 101 (102); *Geminn/Roßnagel*, JZ 2015, 703 (707); *Buchner*, Informationelle Selbstbestimmung, S. 111 ff.; *Eichenhofer*, Der Staat (55) 2016, 41 (43 f.).

[1364] Ausführlich: *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 570 ff.; *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 166 ff.

[1365] Vgl. vertiefend, insbesondere auch zur Begründung der Eingriffsqualität von paternalistischen Einschränkungen: *Sandfuchs*, Privatheit wider Willen, S. 125 ff., 158 ff.; vgl. allgemein *Bosesky/Brüning*, Schutz von digitaler Privatheit, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 88; *Buchholtz*, AöR 2015, 121 (136 ff.); *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 91.

[1366] *Bäcker*, Der Staat (51) 2012, 91 (96); *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 571 ff.

[1367] *Piltz*, Soziale Netzwerke, S. 19 f.; *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 32 ff.; vgl. auch *Roßnagel/Jandt*, MMR 2011, 637 (637 f.).

[1368] *Niemann/Schenk*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 37 f.; *Bäcker*, Der Staat (51) 2012, 91 (96); *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 571 ff..

Volkszählungsurteil postuliert, dass es nicht schrankenlos gewährleistet ist.[1369] Diese Schranken beziehen sich auch und insbesondere auf die Möglichkeiten der Beeinflussung des eigenen Fremdbildes. Niemand hat ein absolutes, uneingeschränktes Herrschaftsrecht über seine Daten, das dazu führen würde, dass er ganz allein entscheiden kann, welche Informationen über ihn einem anderen zugehen und wie diese interpretiert werden. Dies statuiert auch ausdrücklich Erwägungsgrund 4 der DS-GVO. Vielmehr stellen Informationen ein „Abbild sozialer Realität"[1370] dar, die sich erst im Interpretationsprozess verschiedener Beteiligter formen.[1371] Ein Fremdbild kann daher erst im sozialen, kommunikativen Austausch mit anderen entstehen. Würden die anderen Menschen darauf verpflichtet, nur Informationen aus der Hand des sich Darstellenden zu erhalten und keinerlei weitere Informationsquellen über diesen zu nutzen, würden sie in ihrem eigenen Recht auf Meinungs(bildungs-)freiheit verletzt.[1372] Gleichzeitig würde dem Betroffenen das Recht zugewiesen, die Beobachtungen und Sinnkonstruktionen anderer zu beherrschen, ohne dass er dies faktisch jemals ausüben könnte.[1373] Die informationelle Selbstbestimmung bietet „keinen Anspruch auf eine gelingende Selbstdarstellung".[1374]

Die bloße Möglichkeit zur Beschränkung der informationellen Selbstbestimmung anderen gegenüber bietet natürlich noch keine Antwort darauf, wann eine paternalistische Beschränkung der informationellen Selbstbestimmung zum Schutz vor sich selbst zulässig oder gar geboten sein kann. Diese Abwägung ist vielmehr stets in Bezug auf eine konkrete Maßnahme zu treffen, indem die Eingriffsintensität auf ihre Verhältnismäßigkeit überprüft wird. Von Bedeutung ist hierfür insbesondere, wie erheblich das auszugleichende Rationalitätsdefizit ist, ob Dritte durch die Informationspreisgabe betroffen wären und wie groß der Schaden für die durch das Grundgesetz statuierte objektive Werteordnung wäre, wenn eine

[1369] BVerfGE 65, 1, 43 f. – Volkszählung.
[1370] BVerfGE 65, 1 (44).
[1371] *Albers*, Rechtstheorie (33) 2002, S. 68 ff.; *Trute*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 2.5, Rn. 19; *Roßnagel*, in: Ders. (Hrsg.), Hdb. Datenschutzrecht, Kap. 3.4, Rn. 40; vgl. auch *Hoffmann-Riem*, AöR 1998, 513 (521); *Greve*, Drittwirkung, in: FS Kloepfer, S. 671; vgl. auch bereits oben unter B.II.1.
[1372] Vgl. *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 168, 234; *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 571 f.; *Piltz*, Soziale Netzwerke, S. 288; *Masing*, NJW 2012, 2305 (2307); *Bäcker*, Der Staat (51) 2012, 91 (96).
[1373] *Trute*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, Kap. 2.5, Rn. 19; *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 567 f.
[1374] *Britz*, Informationelle Selbstbestimmung, in: *Hoffmann-Riem* (Hrsg.) Offene Rechtswissenschaft, S. 572 m.w.N.; vgl. auch *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 168.

Regelung unterlassen würde.[1375] Soweit sich eine Person umfassend informiert, selbstbestimmt und freiwillig für eine Informationspreisgabe entscheidet, ohne dabei Dritten zu schaden, scheidet eine paternalistische Bevormundung aus.[1376]

Aus der Erkenntnis der Vielschichtigkeit der informationellen Selbstbestimmung folgt daher abstrakt nur, dass paternalistische Regelungen in besonderem Maße rechtfertigungsbedürftig sind und stets auch mit der Beschränkung des kommunikativen Aspekts ebendieses Grundrechts abgewogen werden müssen.

b) „Nudging" als Teil eines liberalen Paternalismus

Sehr streng genommen könnte man bereits das Konzept des Datenschutzes durch Design oder Technik als paternalistisch einstufen, da unabhängig vom konkreten Willen der Nutzer restriktive Standards für die Datenverarbeitung festgelegt werden.[1377] Durch den in soziologischen und verhaltenspsychologischen Versuchen nachweisbaren Status Quo Bias vieler Menschen, der sie zur Beibehaltung einer einmal geschaffenen Situation treibt[1378], kommt dem Konzept eine klare Steuerungswirkung zu, ohne ausdrücklich Freiheiten zu beschränken. Man könnte es daher als einen „Nudge" im Sinne des von *Thaler* und *Sunstein* propagierten liberalen bzw. libertären Paternalismus bezeichnen.[1379] Ein „Nudge" bezeichnet „alle Maßnahmen, mit denen Entscheidungsarchitekten das Verhalten von Menschen in vorhersagbarer Weise verändern können, ohne irgendwelche Optionen auszuschließen oder wirtschaftliche Anreize stark zu verändern".[1380] Er soll zudem leicht zu umgehen sein und ist damit „nur ein Anstoß, keine Anordnung".[1381]

Freilich ist die aus den Standardvorgaben des Datenschutzes durch Design oder Technik folgende Freiheitseinschränkung für den individuellen Nutzer fast schon als trivial zu

---

[1375] *Eidenmüller*, JZ 2011, 814 (815); sehr ausführlich zu dieser Abwägung *Sandfuchs*, Privatheit wider Willen, S. 155 ff.; kritisch zur objektiven Feststellbarkeit von individuellen Rationalitätsdefiziten und hieraus abgeleiteten normativen Handlungsaufträgen *Hermstrüwer*, Informationelle Selbstgefährdung, S.357 ff., welcher als Konsequenz für eine verstärkte Rechtfertigung von paternalistischen Regelungen durch Förderung von Gemeinwohlzielen plädiert.

[1376] *Sandfuchs*, Privatheit, S. 128 ff.; *Kutscha*, GR-Schutz im Internet, S. 11, 47; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 91; vgl. auch *Buchner*, Informationelle Selbstbestimmung, S. 110 ff.; *Karg*, DuD 2013, 75 (78 f.); zu dieser Abwägung auch noch unten unter D.III.4.c)cc).

[1377] Instruktiv zum Begriff des Paternalismus: *Eidenmüller*, JZ 2011, 814 (814) m.w.N.

[1378] Instruktiv: *Thaler/Sunstein*, Nudge, S. 55 ff., 123 ff.; vgl. auch *Wolff*, RW 2015, 194 (199 f.) m.w.N.; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 370 f.

[1379] Instruktiv: *Thaler/Sunstein*, Nudge, S. 9 ff.

[1380] *Thaler/Sunstein*, Nudge, S. 15; kritisch eine dennoch freiheitsbeschränkende und damit rechtfertigungsbedürftige Wirkung aufzeigend *Sandfuchs*, Privatheit wider Willen, S. 223 ff.

[1381] *Thaler/Sunstein*, Nudge, S. 15.

betrachten, solange diese individuell angepasst werden können. Ein niedriges Datenschutzlevel dürfte kaum im Interesse der Mehrheit der Nutzer liegen, insbesondere wenn es um die öffentliche Sichtbarkeit von Profileinträgen, aber auch die Möglichkeit der Weiterverarbeitung der Daten geht. Mit bis zu 1,6 Milliarden anderen Menschen zu kommunizieren und von diesen bewertet zu werden, entspricht im Zweifel nicht der standardmäßigen Absicht eines einzelnen Nutzers und seiner allgemeinen Lebensrealität. Auch mögliche ökonomische Konsequenzen wie die Verteuerung einer Versicherung aufgrund von ungebetener Datenverarbeitung dürften eher selten von Nutzern gewollt sein. Entsprechend handelt es sich tatsächlich nicht so sehr um eine Freiheitsbeschränkung als vielmehr eine Schaffung von Voraussetzungen für selbstbestimmte Freiheitsausübung.[1382] Zudem geht es weniger um eine Änderung des Nutzerverhaltens als vielmehr den Schutz der Nutzer vor von ihnen weder beabsichtigter noch mutmaßlich gewünschter extensiver Datenverarbeitung und Veröffentlichung ihrer Daten.

Der Ansatz des Nudging sieht sich in sozialen Netzwerken darüber hinaus dem grundsätzlichen Problem ausgesetzt, dass der Staat nicht der direkte „Entscheidungsarchitekt" im Sinne von *Thaler* und *Sunstein*[1383] ist. Alle aktuell relevanten und großen sozialen Netzwerke werden von privaten Unternehmen angeboten. Der Staat kann nicht direkt auf die Gestaltung und Nutzung von sozialen Netzwerken Einfluss nehmen und dadurch deren Nutzer in eine gewünschte Richtung steuern, wenn die Gestaltungshoheit in der Hand eines privaten Unternehmens liegt. Der Staat kann lediglich Einfluss auf den Anbieter des sozialen Netzwerks nehmen, um mittelbar das Verhalten der Nutzer zu steuern. Ein idealtypisches staatliches Nudging, das ohne klassische Regulierungselemente insbesondere in Form von ordnungsrechtlichen Vorgaben auskommt, ist daher nicht möglich.

Staatliche Regulierung der Anbieter sozialer Netzwerke würde aber regelmäßig kein Nudging darstellen. Die Ausgangsprämisse des Nudging ist, dass es Rationalitätsdefizite von Menschen ausgleichen soll.[1384] Die besonders strenge Auslegung nach *Thaler* und *Sunstein* geht dabei von einem Idealbild des *homo oeconomicus* aus, von welchem die meisten Menschen abweichen; *Thaler* und *Sunstein* bezeichnen diese Menschen als „Humans".[1385] Ihnen stehen die „Econs" gegenüber, die ihre Entscheidungen stets wirtschaftlich rational treffen und daher nicht den

[1382] So auch bereits *Sandfuchs*, Privatheit wider Willen, S. 169 f.
[1383] *Thaler/Sunstein*, Nudge, S. 11, 23 ff.
[1384] *Thaler/Sunstein*, Nudge, S. 16 ff.; kritisch zur Übertragbarkeit auf das Datenschutzrecht *Hermstrüwer*, Informationelle Selbstgefährdung, S. 359 ff.
[1385] *Thaler/Sunstein*, Nudge, S. 16 f.

vermeintlichen Rationalitätsdefiziten unterliegen.[1386] *Thaler* und *Sunstein* räumen selbst ein, dass Nudges gegenüber Econs ins Leere laufen, da diese die mit den Nudges verbundene Manipulation entweder durchschauen oder aber bereits unabhängig von diesen die entsprechende Entscheidung getroffen hätten. Tatsächlich ist es Teil ihrer Definition eines Nudge, dass er von Econs ignoriert würde.[1387]

Im Rahmen dieser Unterscheidung sind die Anbieter sozialer Netzwerke als Econs zu klassifizieren. Nach der strengen Theorie von *Thaler* und *Sunstein* scheint es ausgeschlossen, dass Nudging gegenüber diesen Akteuren Wirkung zeigen könnte, da sie als Econs die Nudgingmaßnahmen als solche durchschauen und sich daher nicht von ihnen beeinflussen lassen würden bzw. auch ohne die Maßnahme das gewünschte Verhalten gegebenenfalls gezeigt hätten. Es würde sich daher jedenfalls nicht um Nudging im engeren Sinne handeln, da die Anbieter sehr gezielt auf die staatlichen Maßnahmen wie etwa Steuererleichterungen reagieren würden und diese auch bewusst wahrnehmen und analysieren könnten.

Auch bei einer weicheren Abgrenzung anhand eines anderen Rationalitätsmaßstabes wie etwa dem eines mündigen Verbrauchers ist es jedenfalls zweifelhaft, ob staatliche Maßnahmen gegenüber den Anbietern sozialer Netzwerke als Nudging einzustufen wären. Sie kompensieren in keinem Fall Rationalitätsdefizite der Anbieter, sondern setzen nur Anreize zur Verwirklichung und Einhaltung staatlicher Ziele und Wertvorstellungen. Letztendlich handelt es sich damit ganz ohne Rückgriff auf das Konzept des Nudging um Steuerungsinstrumente im Sinne der Neuen Verwaltungsrechtswissenschaft.[1388]

Diese Instrumente beziehen ihre Wirksamkeit aber gerade nicht aus einer unbemerkten Manipulation in Form einer gezielten Entscheidungsarchitektur und damit einer nur –

[1386] *Thaler/Sunstein*, Nudge, S. 17, 31 ff.; kritisch *Wolff*, RW 2015, 194 (210 ff.) m.w.N. unter Verweis darauf, dass im Rahmen langfristiger menschlicher Interaktion auch ökonomisch vermeintlich irrationales Verhalten zu sozialen Vorteilen führen könne und damit der *homo oeconomicus* nicht zwingend ein überlegenes Rationalitätsmodell darstelle; kritisch auch *Eidenmüller*, JZ 2011, 814 (819 ff.), da sich aus dem bloßen Vorliegen von Rationalitätsdefiziten noch kein normativer Maßstab ergebe, wie diese aufzulösen seien, und dem liberalen Paternalismus damit eine normative rechtspolitische Konzeption fehle. *Hermstrüwer*, Informationelle Selbstgefährdung, S. 348 ff. weist kritisch darauf hin, dass die dem Modell zugrundeliegende *Rational Choice* Theorie nur unzureichend bewusstes Verhalten aufgrund zeitinkonsistenter (sozialer) Präferenzen abbilde und derartiges Verhalten vorschnell als rechtlich zu korrigierende kognitive Verzerrung bzw. als Rationalitätsdefizit einordne.

[1387] *Thaler/Sunstein*, Nudge, S. 19. Diese Voraussetzung ist freilich dann nicht zwingend, wenn man einen anderen Rationalitätsmaßstab als den *homo oeconomicus* anlegt – beispielsweise den eines mündigen Verbrauchers – und damit die Gruppen der Humans und der Econs realistischer und undogmatischer ansetzt.

[1388] Vgl. auch bereits *Eidenmüller*, JZ 2011, 814 (820); *Wolff*, RW 2015, 194 (205 ff.); instruktiv zur Neuen Verwaltungsrechtswissenschaft: *Voßkuhle*, Neue Verwaltungsrechtswissenschaft, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR I, § 1, Rn. 16 ff. m.w.N.; vgl. auch *Fehling*, Informelles Verwaltungshandeln, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II, § 38 Rn. 43 ff.

vermeintlich – minimalen Freiheitseinschränkung. Die Wirksamkeit von niederschwelligen Steuerungsmaßnahmen des Staates liegt vielmehr in der abstrakten Drohung begründet, im Falle einer Nichtbefolgung strengere Regulierungsformen etwa im Sinne von klassischen ordnungsrechtlichen Vorschriften einzusetzen. Somit läge aber gerade kein liberaler Paternalismus und auch kein Nudging im eigentlichen Sinne vor.

Effektive staatliche Nudgingmaßnahmen zur Förderung der informationellen Selbstbestimmung von Nutzern in sozialen Netzwerken sind somit – unabhängig von ihrer grundsätzlichen Legitimität[1389] – kaum vorstellbar. Da der Staat nicht selbst Entscheidungsarchitekt ist, kann er nicht direkt Nudgingmaßnahmen gegenüber den Nutzern einsetzen; dies ist den Anbietern sozialer Netzwerke vorbehalten. Eine staatliche Einflussnahme auf das Nutzerverhalten ist folglich nur durch Vorgaben gegenüber den Anbietern sozialer Netzwerke möglich, das soziale Netzwerk in einer bestimmten Form zu gestalten. Hierbei wird es sich aber regelmäßig nicht um Nudging handeln, sondern um klassische ordnungsrechtliche Regulierung und ggf. niederschwellige staatliche Steuerungsmaßnahmen. Es bestünde daher im Wesentlichen eine Deckungsgleichheit zu den bereits unter D.III.3. diskutierten und nun unter c) zu diskutierenden Maßnahmen und den dort auftretenden Fragen der Verhältnismäßigkeit.

c) Zugangsbeschränkungen und Verbote

Klassische staatliche Regulierungsmaßnahmen zum Schutz der Nutzer vor sich selbst könnten insbesondere in Form von Zugangsbeschränkungen zu sozialen Netzwerken erlassen werden. Hierbei ist sowohl an eine allgemeine Zugangsbeschränkung gleichsam im Sinne eines Internetführerscheins zu denken, als auch an Altersgrenzen für Minderjährige. Zudem stellt sich die Frage nach der Angemessenheit spezifischer Verbote für (selbst-)gefährdende Handlungen.

aa) Ein ‚Führerschein' für soziale Netzwerke?

Man könnte überlegen, die Zulässigkeit der Nutzung von sozialen Netzwerken davon abhängig zu machen, dass der Nutzer nachweisen kann, sich zuvor hinreichend über die Risiken einer

[1389] Vgl. hierzu bereits kritisch *Hermstrüwer*, Informationelle Selbstgefährdung, S. 359 ff., welcher anführt, dass der liberale Paternalismus im Allgemeinen und das Nudging im Speziellen letztlich eine Wohlfahrtsmaximierung bezweckten, was aber allenfalls ein sekundärer Zweck des Datenschutzrechts sei: Es fehle an einer Begründung, warum „die Maximierung individueller Wohlfahrt verfassungsrechtlich stärker zu gewichten ist als die individuelle Freiheit zur beschränkt rationalen Selbstgefährdung.", a.a.O., S. 362, m.w.N.; ablehnend auch *Sandfuchs*, Privatheit wider Willen, S. 223 ff..

solchen Nutzung informiert zu haben. Eine solche Beschränkung könnte dazu beitragen, dass soziale Netzwerke bewusster und vorsichtiger genutzt werden.

Dem stehen indes zwei große Probleme entgegen: Zum einen ist sehr fraglich, ob diese Maßnahme den gewünschten Effekt erzielen würde. Zum anderen könnte eine ungerechtfertigte zeitliche und finanzielle Zugangshürde zu sozialen Netzwerken geschaffen werden.

Freilich hängt viel davon ab, wie ein entsprechender Nachweis zu erlangen wäre. Das verpflichtende Anschauen eines Onlinevideos und die Beantwortung eines kurzen Multiplechoice-Testes im Anschluss – eventuell gar mit beliebig vielen Versuchen – würde zwar leicht durchführbar und kostengünstig sein. Allerdings darf bezweifelt werden, ob dies zu einer nachhaltigen Problemeinsicht und größerer Vorsicht führen würde. Eine verpflichtende Teilnahme an Seminaren und Unterrichtsstunden, zusammen mit einer offiziellen, vielleicht gar staatlichen Prüfung wäre dagegen schnell mit einem erheblichen Aufwand und wohl auch nicht geringen Kosten verbunden, ohne dabei eine Garantie für die nachhaltige Wirkung bieten zu können. Personen ohne die entsprechenden zeitlichen oder finanziellen Möglichkeiten bliebe damit der Zugang zu einem in der heutigen Gesellschaft sehr wichtigen Kommunikationsmedium verwehrt, was einen schweren Eingriff in ihre Rechte darstellen würde.[1390]

Selbst wenn sich ein Testverfahren finden ließe, das weder eine zu große Hürde aufbaut, noch so leicht zu überwinden ist, dass es nicht ernstgenommen wird, bliebe das Problem der Identifikation des Nutzers und des Nachweises der erworbenen Kompetenz.[1391] Anders als in einer persönlichen Führerscheinkontrolle lässt sich im Internet nicht direkt überprüfen, wer vor dem Computer sitzt und eine Anfrage startet. Eine Aufforderung zur einfachen Bestätigung, dass man den geforderten Test zur Nutzung des sozialen Netzwerks bestanden hat, wäre zweifellos eine höchst ineffektive Sicherungsmaßnahme, da es an geeigneten Sanktions- und Feststellungsmechanismen bei Falschangaben fehlt. Aber auch eine Verifikation durch einen Code, den man nur bei Bestehen des Tests erhält, ist im Ergebnis keine effektive Lösung, da kaum verhindert werden kann, dass dieser Code in fremde Hände gerät, sei es durch freiwillige Weitergabe oder durch illegales Hacking.[1392]

[1390] Vgl. zur gesellschaftlichen Bedeutung von sozialen Netzwerken bereits oben unter B.I.2; vgl. instruktiv zum grundrechtlichen Teilhabeanspruch *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Rn. 57 ff.

[1391] Vgl. zur Identitätsfeststellung im Internet *Roßnagel/Hornung*, DÖV 2009, 301 (302 f.).

[1392] Vgl. allgemein *Roßnagel/Hornung*, DÖV 2009, 301 (302 f.).

Eine effektive Verifikation ließe sich beispielsweise erreichen, wenn allen Bürgern ein Code zugeteilt würde, der generell für die Identifikation im Internet genutzt und amtlich mit gewissen Daten über den Bürger wie Name, Alter und eben möglicherweise dem Bestehen eines entsprechenden Testes verknüpft werden könnte.[1393] Die große Bedeutung eines solchen Codes würde wohl zumindest die freiwillige Weitergabe weitgehend eindämmen, wie dies auch bei PIN-Codes der Fall ist. Tatsächlich besteht mit dem neuen elektronischen Personalausweis auch bereits eine Infrastruktur, um eine solche Verifikation zu ermöglichen.[1394]

Die Etablierung eines derartigen Verifikationsmechanismus könnte indes eine deutliche Einschränkung des Rechts auf anonyme Internetnutzung gemäß § 13 Abs. 6 TMG bedeuten, da zumindest der Staat theoretisch die Nutzung zurückverfolgen könnte. Zwar besteht gegenüber den Anbietern sozialer Netzwerke – nach hier vertretener Auffassung – ohnehin kein Anspruch auf eine anonyme Registrierung. Zudem ist es technisch möglich, dem Anbieter des sozialen Netzwerks nur Zugriff auf bestimmte Teile dieses digitalen Personalausweises zu ermögliche. Im Rahmen von Verschlüsselungsverfahren könnte beispielsweise sichergestellt werden, dass der Anbieter aus dem übertragenen Code zwar ersehen kann, ob die das Netzwerk nutzende Person die notwendige Qualifikation aufweist, nicht aber nicht auf sonstige personenbezogene Daten zugreifen könnte.[1395]

Dennoch können gegen eine solche Lösung erhebliche Missbrauchsbedenken angemeldet werden.[1396] Es macht einen bedeutenden Unterschied, ob es lediglich die freiwillige Möglichkeit gibt, einen elektronischen Personalausweis zu nutzen, oder ob die Nutzung zur Voraussetzung für die Inanspruchnahme von gesellschaftlich bedeutsamen Internetdienstleistungen wie sozialen Netzwerken gemacht wird. Bereits heute sind Identitätsdiebstahl und das Hacken von vertraulichen Identifikationsmechanismen, etwa PIN-Codes und Passwörtern, bekannte und verbreitete Probleme.[1397] Sollte ein elektronischer Personalausweis gehackt werden, können der betroffenen Person schwerwiegende Probleme drohen, die noch weit über die heutigen Konsequenzen eines Identitätsdiebstahls, die vor allem auf kommerzielle Aspekte beschränkt sind, hinausgehen. Insbesondere erschwerte sich der

[1393] Im Rahmen eines Verfahrens zur Altersverifikation wird vorgeschlagen, hierfür den elektronischen Personalausweis zu benutzen, vgl. *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 386.
[1394] Vgl. zum elektronischen Personalausweis ausführlich *Roßnagel/Hornung*, DÖV 2009, 301 (303 ff.).
[1395] Diese Funktionen zur pseudonymen Nutzungsmöglichkeit sind bereits heute im elektronischen Personalausweis enthalten, vgl. *Roßnagel/Hornung*, DÖV 2009, 301 (304).
[1396] Vgl. allerdings ausführlich zu technischen Sicherungsmaßnahmen *Hornung*, Die digitale Identiät, S. 346 ff.; *Borges*, NJW 2010, 3334 (3337 f.).
[1397] Vgl. *Gercke*, ZUM 2012, 625 (630 f.).

Nachweis, eine bestimmte Tat im Internet nicht begangen zu haben, wenn ein solcher Identifikationscode missbraucht würde.[1398] Während der elektronische Personalausweis somit zwar gegenwärtig sicherer gestaltet werden kann als sonstige gängige Identifikationsverfahren im Internet[1399], wäre das Schadenspotential angesichts der umfassenden Legitimationswirkung erheblich größer, sollte es doch zu einem Missbrauch der Daten kommen.

Zudem würde die Einführung eines persönlichen Identifikationscodes als Voraussetzung für die Nutzung von Internetdienstleistungen eine Infrastruktur für eine totale digitale Überwachung schaffen. Die gegenwärtigen indirekten Identifikationsmechanismen wie die IP-Adresse würden ersetzt durch eine direkt personenbezogene Kontrolle, wer einen bestimmten Dienst, etwa ein soziales Netzwerk, nutzt. Dies ist freilich gerade der vorhin erwünschte Vorteil. Es fällt aber nicht schwer, sich mögliche staatliche und private Missbrauchsmöglichkeiten einer solchen Infrastruktur vorzustellen. So wäre es nur ein kleiner Schritt, die Anwendungsbereiche eines solchen Identifikationscodes von einzelnen Diensten sukzessive auf das gesamte Internet auszudehnen. Hiermit würden die Voraussetzungen einer kaum umgehbaren staatlichen Überwachung individuellen Verhaltens im Internet geschaffen. Angesichts der andauernden Diskussion um die Vorratsdatenspeicherung ist es jedenfalls nicht unplausibel, dass es Bestrebungen geben würde, diese Überwachungsinfrastruktur auch entsprechend zu nutzen. Ebenso würde es für private Unternehmer noch sehr viel leichter, Nutzer im Internet zu überwachen und Persönlichkeitsprofile über sie zu erstellen. Anstatt Nutzer über Cookies, Browser-IDs und ähnliche Trackingmethoden zu verfolgen, könnte gegebenenfalls direkt auf den Identifikationscode zurückgegriffen werden.

Missbrauchsmöglichkeiten stellen freilich nur in dem Maße relevante Argumente dar, wie sie realistisch zu erwarten sind, wie groß die aus ihnen resultierenden Schäden wären und wie zuverlässig sie sich durch Verfahrensvorschriften eindämmen oder ausschließen lassen. Eine anlasslose staatliche Totalüberwachung individuellen Verhaltens im Internet würde eine massive Verletzung von Grundrechten darstellen und wäre daher ein sehr erheblicher Schaden.[1400] Wenngleich unter dem Eindruck der terroristischen Anschläge des 21. Jahrhunderts eine immer stärkere Beschneidung von Freiheitsrechten zugunsten einer vermeintlichen Sicherheit erfolgt ist[1401], ist ein Missbrauch solchen Ausmaßes unter Geltung

[1398] Vgl. hierzu *Borges*, NJW 2010, 3334 (3338 f.).
[1399] *Roßnagel/Hornung*, DÖV 2009, 301 (303 f.).
[1400] Vgl. BVerfGE 120, 274 (321 ff.) – Onlinedurchsuchung.
[1401] Vgl. für eine ausführliche Darstellung *Buchner*, Informationelle Selbstbestimmung, S. 68 ff. m.w.N.

des Grundgesetzes daher dennoch sehr unwahrscheinlich.[1402] Schwerer wiegen entsprechend private und kriminelle Missbrauchsmöglichkeiten.

Letztendlich handelt es sich bei der Einführung eines persönlichen Identifikationscodes im Internet um eine Debatte, die in ihrer Bedeutung weit über die Nutzung von sozialen Netzwerken hinausgeht. Sie kann an dieser Stelle daher weder abschließend dargestellt noch gar entschieden werden. Im Gesamtkontext der Einführung eines solchen Identifikationscodes stellt sich der Anwendungsbereich in sozialen Netzwerken jedenfalls als ein bloßer Nebenschauplatz dar. Entsprechend sollte über seine Einführung auch nur im Rahmen des größeren Kontexts diskutiert werden und eine Einführung nicht vorschnell aufgrund möglicher Vorteile in einem kleinen Bereich gefordert werden.

Eine allgemeine Zugangsbeschränkung zu sozialen Netzwerken durch das Erfordernis einer Art von Führerschein kann daher ein grundsätzlich geeignetes Mittel sein, um dort auftretende Gefahren für die informationelle Selbstbestimmung der Nutzer zu reduzieren. Dies gilt aber nur, wenn ein effektiver Nachweis über die erfolgte Aufklärung gelingt, damit es nicht zu Umgehungen kommt und die Aufklärung auch ernstgenommen wird. Die Schaffung der Voraussetzungen eines solchen Nachweises würde aber auch einen großen Schritt in Richtung einer umfassenden Überwachungsinfrastruktur darstellen. Zudem können sich aus dem notwendigen Testverfahren finanzielle und zeitliche Hürden ergeben, die Personen von der Nutzung sozialer Netzwerke ausschließen können. Aufgrund der Vielschichtigkeit der informationellen Selbstbestimmung würde dies zugleich eine Beschränkung derselben bedeuten, wie oben bereits dargelegt.

Angesichts dieser Beschränkungen und den noch sehr offenen Fragen der Missbrauchsbegrenzung eines persönlichen Identifikationscodes für das Internet ist die Einführung einer solchen allgemeinen Zugangsbeschränkung zum gegenwärtigen Zeitpunkt als unverhältnismäßig und nicht empfehlenswert einzustufen.

bb) Altersbeschränkungen

Eine weitere Form der Zugangsbeschränkung ist ein Mindestalter für die Nutzung von sozialen Netzwerken. Viele soziale Netzwerke praktizieren dies bereits über ihre Nutzungsbedingungen. Verbreitet wird hierbei ein Mindestalter von 13 Jahren festgesetzt, teilweise auch ein noch

[1402] Daher die Einführung des elektronischen Identifizierungsnachweis begrüßend *Borges*, NJW 2010, 3334 (3339); *Roßnagel/Hornung*, DÖV 2009, 301 (303 ff.); *Hornung*, Die digitale Identiät, S. 37 ff.

höheres Alter verlangt.[1403] Ob dies praktisch eingehalten wird, ist freilich angesichts der Tatsache sehr fraglich, dass bereits 9-13 Jährige angeben, regelmäßig Facebook zu nutzen.[1404]

Weder in den deutschen Datenschutzgesetzen noch der bisherigen DSRL von 1995 findet sich eine ausdrückliche Regelung eines Mindestalters; auf ihrer Grundlage kann allenfalls die Frage nach der Einwilligungsfähigkeit Minderjähriger in die Datenverarbeitung gestellt werden.[1405] Der bereits erwähnte Streit über die Rechtsnatur der Einwilligung erhält hier praktische Relevanz, da es von seiner Entscheidung abhängt, ob es für die Wirksamkeit der Erklärung auf eine tatsächliche Einsichtsfähigkeit ankommt oder auf die Geschäftsfähigkeit des Minderjährigen. Herrschend wird hier in zutreffender Weise auf die tatsächliche Einsichtsfähigkeit abgestellt.[1406]

Art. 8 Abs. 1 DS-GVO schreibt nunmehr ein Mindestalter von 16 Jahren fest, welches durch mitgliedstaatliche Regelung auf 13 Jahre abgesenkt werden kann. Unterhalb dieser Altersschwelle soll eine datenschutzrechtliche Einwilligung nur mit Zustimmung der gesetzlichen Vertretungsberechtigten erklärt werden können. Freilich wird diese Vorschrift dadurch relativiert, dass der Datenverarbeiter lediglich „angemessene Anstrengungen" unternehmen soll, um sicherzustellen, dass eine solche Zustimmung erteilt wurde.[1407]

[1403] Für ein Mindestalter von 13 Jahren vgl. z.B. Facebook Nutzungsbedingungen Punkt 4 Nr. 5 (https://www.facebook.com/legal/terms (Stand 30. Januar 2015)); MySpace Punkt 1c) der AGB, wo zusätzlich bei einem Alter unter 18 eine Nutzung nur mit Einwilligung der Erziehungsberechtigten gestattet wird (https://myspace.com/pages/terms (Stand 27. April 2017)); Google + im Rahmen eines Googlekontos (https://support.google.com/accounts/answer/1350409?hl=de), wobei in Spanien und Südkorea ein Mindestalter von 14 Jahren, in den Niederlanden von 16 Jahren verlangt wird; Snapchat verbietet in seinen Nutzungsbedingungen unter Punkt 1 ausdrücklich Personen unter 13 Jahren die Erstellung von Accounts (https://www.snap.com/de-DE/terms/#terms-row (Stand 26.9.2017)); die Netzwerke StudiVZ und MeinVZ verlangen ein Mindestalter von 16 Jahren, vgl. jeweils Punkt 2.1 der AGB (http://www.studivz.net/l/terms; http://www.meinvz.net/l/terms); das beruflich orientierte soziale Netzwerk LinkedIn statuierte in seinen Nutzungsbedingungen mit Stand vom 23.10.2014 ebenfalls als grundsätzliches Mindestalter 13 Jahre, für verschiedene Länder aber auch ein höheres Alter, etwa 14 Jahre in Deutschland, 16 Jahre in den Niederlanden und 18 Jahre in der Volksrepublik China; in seinen aktuellen Nutzungsbedingungen verlangt LinkedIn ein pauschales Mindestalter von 16 Jahren, sofern nicht gesetzlich ein höheres Mindestalter gefordert wird, vgl. Punkt 2.1 der AGB (https://www.linkedin.com/legal/user-agreement?trk=uno-reg-guest-home-user-agreement, Stand 7. Juni 2017); das soziale Netzwerk Xing macht die Volljährigkeit zur Nutzungsvoraussetzung, vgl. Punkt 2.4 der AGB (https://www.xing.com/terms#a-2, (Stand 1. April 2017)).

[1404] *DIVSI*, U25-Studie v. Februar 2014, S. 69 ff.

[1405] *Gola/Schulz*, ZD 2013, 475 (475 f.); *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 136 f.; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 336 f.

[1406] *Däubler*, in: DKWW, § 4a BDSG, Rn. 5 m.w.N.; *Simitis*, in: Simitis, BDSG, § 4a Rn. 20 ff. m.w.N., welcher die Einwilligung zwar als rechtsgeschäftliche Erklärung einstuft, aber dennoch die tatsächliche Einsichtsfähigkeit ausreichen lässt; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 95; a.A. *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 137 f., mit dem kritischen Verweis darauf, dass eine individuelle Überprüfung der Einsichtsfähigkeit praktisch nicht umsetzbar ist.

[1407] Kritisch insoweit *Nebel/Richter*, ZD 2012, 407 (410); *Kipker/Voskamp*, DuD 2012, 737 (741).

Angesichts der bisherigen Praxis, ein entsprechendes Mindestalter in den Geschäftsbedingungen festzuschreiben, dürfte die Vorschrift keine großen Veränderungen für die Nutzung sozialer Netzwerke bedeuten.[1408]

Art. 8 Abs. 3 DS-GVO stellt klar, dass die Regelung keine Auswirkungen auf die zivilrechtliche Wirksamkeit eines eventuell abgeschlossenen Nutzungsvertrags hat, sondern insoweit die mitgliedstaatlichen Regelungen im Zivilrecht anwendbar bleiben.

Zivilrechtlich wird in diesem Zusammenhang darüber diskutiert, ob der Nutzungsvertrag eines sozialen Netzwerks von beschränkt Geschäftsfähigen ohne Zustimmung ihrer Eltern geschlossen werden kann und welche Konsequenzen aus einer Unwirksamkeit des Vertrags resultieren.[1409] Da mit Abschluss des Nutzungsvertrags dem Anbieter in aller Regel umfassende Rechte eingeräumt werden, die Nutzerdaten zu verwenden, und vom Gesetz abweichende AGBs vereinbart werden können, erweist sich die Willenserklärung auf Abschluss des Nutzungsvertrags nicht als rechtlich lediglich vorteilhaft.[1410] Auch ein „Bewirken mit eigenen Mitteln“ nach § 110 BGB scheidet regelmäßig aus, da angesichts der fortwährenden Datenpreisgabe niemals von einer vollständigen Bewirkung auszugehen ist. Nutzungsverträge, die zwischen einem Minderjährigen und dem Anbieter eines sozialen Netzwerks geschlossen werden, sind daher regelmäßig schwebend unwirksam gemäß § 108 Abs. 1 BGB.[1411] Sie bedürfen damit der Zustimmung eines gesetzlichen Vertreters. Die Zustimmung ist ausdrücklich zu erteilen, um den Minderjährigenschutz nicht zu unterlaufen.[1412]

Problematisch ist hierbei natürlich, wie die Zustimmungserklärung des gesetzlichen Vertreters durch den Anbieter des sozialen Netzwerks verifiziert werden kann. Allgemeinen zivilrechtlichen Grundsätzen entsprechend liegt es indes im Verantwortungsbereich des Anbieters, hierfür eine effektive (technische) Lösung zu finden.[1413] Dies entspricht auch der Wertung des Art. 8 Abs. 2 DS-GVO für die datenschutzrechtliche Einwilligung.

[1408] Ausführlich *Gola/Schulz*, ZD 2013, 475 (476 ff.); *Kipker/Voskamp*, DuD 2012, 737 (739 f.).

[1409] Für eine ausführliche Darstellung vgl. *Piltz*, Soziale Netzwerke, S. 53 ff.

[1410] *Piltz*, Soziale Netzwerke, S. 53 f.; *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 137 f.; *Jandt/Roßnagel*, MMR 2011, 637 (639); *Bräutigam*, MMR 2012, 635 (637).

[1411] Ausführlich: *Piltz*, Soziale Netzwerke, S. 55 ff.; *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 137 f.; vgl. auch *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 338 f.

[1412] *Piltz*, Soziale Netzwerke, S. 54 f.; *Jandt/Roßnagel*, MMR 2011, 637 (640); a.A. *Bräutigam*, MMR 2012, 635 (638), der auch eine konkludente Einwilligung anhand konkreter Anhaltspunkte ausreichen lassen will, nicht aber eine generelle Erlaubnis, das Internet zu verwenden.

[1413] Vgl. zur Risikoverteilung nach den §§ 106 ff. BGB instruktiv *Schmitt*, MüKo-BGB, Bd. 1, § 106 BGB, Rn. 18.

Eine Altersbeschränkung für die Nutzung sozialer Netzwerke ist sicherlich eine begrüßenswerte und sinnvolle Maßnahme.[1414] Die Langfristigkeit und Verbreitungsmöglichkeiten von Daten und Informationen im Internet sind für Kinder nur sehr schwer zu erfassen, so dass kaum von einer eigenverantwortlichen Datenpreisgabe ausgegangen werden kann.[1415] Weiterhin besteht für alle Nutzer eine gewisse Verantwortung, sich in der kommunikativen Situation, die soziale Netzwerke per definitionem darstellen, angemessen und verantwortungsbewusst zu verhalten. Es kann bezweifelt werden, dass 13- bis 18-Jährige bereits ein hinreichendes Verantwortungsbewusstsein aufweisen, um dieser Herausforderung umfassend gerecht zu werden.[1416] Gerade tragische Fälle von Mobbing in sozialen Netzwerken, die im Extremfall zu Selbstmorden führen können[1417], weisen darauf hin, wie folgenreich unverantwortliche Kommunikation in sozialen Netzwerken und allgemein im Internet sein kann. Soziale Netzwerke können für persönliche Rachefeldzüge genutzt werden und an jeglicher Rechtsstaatlichkeit vorbei öffentliche Verurteilungen durch einen sogenannten Shitstorm erzeugen. Die einfache, oft ungeprüfte Weiterleitung von Aussagen führt zu einem digitalen Pranger, an dem Individuen vorgeführt werden können.[1418] Die Einführung eines Mindestalters erhöht insofern die Chancen eines verantwortungsbewussten Umgangs und schützt jüngere Kinder gegen entsprechende Formen des ‚Cybermobbings'.

Zuletzt kann in sozialen Netzwerken auch immer das Risiko des Kindesmissbrauchs durch Sexualstraftäter bestehen.[1419] Profile von Kindern mit sehr freizügigen Privatsphäre-Einstellungen, in denen beispielsweise Fotos und Adressen enthalten sind, erlauben eine gezielte Suche nach potentiellen Opfern und eine direkte Ansprache. Soziale Netzwerke versuchen derartige Kontaktaufnahmen freilich in ihren Nutzungsbedingungen vertraglich zu unterbinden. Beispielsweise verbietet Facebook es verurteilen Sexualstraftätern, sich ein Nutzerkonto anzulegen.[1420] Solche Regelungen können indes immer nur einen begrenzen

---

[1414] Gar für eine staatliche Pflicht zur Einführung und Durchsetzung einer Altersgrenze und –verifikation plädieren *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S.334 ff., 386.

[1415] *v. Zimmermann*, Einwilligung, S. 164; *Buchner*, Informationelle Selbstbestimmung, S. 248; *Kutscha*, GR-Schutz im Internet, S. 46; OLG Hamm, DuD 2013, 106 ff., welches sogar noch für Minderjährige ab dem 15. Lebensjahr Zweifel an der Einwilligungsfähigkeit hegt; *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 340.

[1416] *Roßnagel*, Persönlichkeitsentfaltung, in: Bieber/Eifert (u.a.) (Hrsg.), Soziale Netze in der digitalen Welt, S. 278; *Jandt/Roßnagel*, MMR 2011, 637 (641 f.); *Bräutigam*, MMR 2012, 635 (637 f.); vgl. auch *Maisch*, Informationelle Selbstbestimmung, S. 193 ff.

[1417] Vgl. *Heckmann*, NJW 2012, 2631 (2632); *Kutscha*, GR-Schutz im Internet, S. 14; *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, S. 78.

[1418] *Jandt/Roßnagel*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre, S. 318 ff.; *Kutscha*, GR-Schutz im Internet, S. 14.

[1419] Vgl. *Caspar*, ZRP 2015, 233 (236).

[1420] Punkt Nr. 4.6 der Nutzungsbedingungen, https://www.facebook.com/legal/terms (Stand 30. Januar 2015).

Schutz für Kinder bieten, während sie zugleich eine erhebliche Einschränkung für ehemalige Täter auch lange nach Verbüßung ihrer staatlichen Strafe bedeuten. Sie entfalten zudem keinerlei Schutzwirkung gegenüber Ersttätern oder noch nicht verurteilten Tätern.

Zum Schutz von Kindern ist es daher sehr zu begrüßen, dass zukünftig nur noch eine mit den Erziehungsberechtigten abgestimmte Nutzung sozialer Netzwerke rechtlich zulässig sein wird. Da eine individuelle Überprüfung der Einsichtsfähigkeit im Internet nicht praktikabel ist, ist eine starre Altersgrenze hierbei klar vorzugswürdig.[1421] Die faktisch bereits häufig verwendete und nunmehr in Art. 8 Abs. 1 DS-GVO vorgesehene Grenze von 16 und mindestens 13 Jahren stellt insoweit einen guten Kompromiss zwischen dem Schutz von Kindern und der Ermächtigung von Jugendlichen dar, sich kommunikativ zunehmend unabhängig und selbstständig zu entfalten. Unterstützend sollten allerdings verpflichtende, besonders restriktive Privatsphäre-Einstellungen für alle Nutzer von sozialen Netzwerken unter 18 Jahren gelten, um einen besonders hohen Schutz zu gewährleisten. Einige Funktionen könnten für Profile von Minderjährigen auch gänzlich deaktiviert werden, etwa die Möglichkeit, das Profil im sozialen Netzwerk öffentlich zu schalten.

Unabhängig von dieser rechtlichen Betrachtung stellt sich aber bei jedem Vollzug von Altersgrenzen das gleiche Problem der zuverlässigen Verifikation[1422], das bereits für eine allgemeine Zugangsbeschränkung im Sinne eines „Internetführerscheins“ erläutert wurde. Eine Lösung hierfür muss dem politischen Prozess und der technischen Innovation vorbehalten bleiben.

cc) Verbote bestimmter Informationspreisgaben

Eine weniger einschneidende Maßnahme als eine vollständige Zugangsbeschränkung wäre ein Verbot von bestimmten Einzelhandlungen in sozialen Netzwerken bzw. eine Reduzierung von möglichen Handlungsoptionen. Zu differenzieren ist hier nach Verboten, die Dritte schützen sollen, und Verboten, die dem Schutz des Nutzers ‚vor sich selbst‘ dienen. Unstreitig ist, dass die normalen Gesetze auch im Internet und damit in sozialen Netzwerken gelten; das Internet ist gerade kein ‚rechtsfreier Raum‘. Soweit es daher um Verbote geht, die beispielsweise durch die Tatbestände der Beleidigung (§§ 185 ff. StGB), des Stalkings (§ 238 StGB), des Betrugs

[1421] So auch *v. Zimmermann*, Einwilligung, S. 180; vgl. auch *Jandt/Roßnagel*, MMR 2011, 637 (640). *Maisch*, Informationelle Selbstbestimmung, S. 195 f. betont hingegen die Bedeutung der Einsichtsfähigkeit Minderjähriger im konkreten Einzelfall und spricht sich daher gegen abstrakte Altersgrenzen für die Nutzung sozialer Netzwerke aus.

[1422] Vgl. hierzu auch *Jandt/Roßnagel*, MMR 2011, 637 (641).

(§§ 263, 263a StGB) oder – angesichts der Flüchtlingskrise sehr aktuell – der Volksverhetzung (§ 130 StGB) aufgestellt werden, steht außer Frage, dass entsprechende Handlungen auch in sozialen Netzwerken nicht zulässig sind.[1423]

Inwieweit Verbote oder Einschränkungen erlassen werden können, die ausschließlich dem Schutz des Nutzers ‚vor sich selbst' dienen, wurde kritisch von *Sandfuchs* in ihrer unlängst erschienenen Dissertation untersucht.[1424] Eine entsprechende konkrete Maßnahme in sozialen Netzwerken wäre es beispielsweise, Datenpreisgaben oder Handlungen, die abstrakt zu langfristigen Freiheitsgefährdungen führen können, präventiv zu verbieten; etwa ein Verbot, seine private Adresse zu veröffentlichen oder intime Fotos hochzuladen.

Auch hierbei ist – in noch weit größerem Maße als bei Zugangsbeschränkungen –zweifelhaft, ob derartiger Paternalismus nicht über das Ziel hinausschießt und am Ende zu mehr Freiheitseinschränkung führt als er Freiheitsgewinn sichert. Informationelle Selbstbestimmung als Recht auf Selbstdarstellung und Mitteilungsfreiheit schließt das Recht auf einen offenen Umgang mit den eigenen Daten ein. Es ist nicht die Aufgabe des Staates, seine Bürger zu grundsätzlich ‚vernünftigem' Verhalten zu erziehen, sondern allenfalls einen Rahmen zu schaffen, in welchem die Menschen ihre Freiheiten ausleben können.[1425] Für ein bloß selbstgefährdendes Verhalten, das keine anderen Rechtsgüter bedroht und keinen Schaden für Dritte bedeutet, steht dem Staat weder ein Strafanspruch noch ein Recht auf ordnungspolitisches Einschreiten zu.[1426] Es ist daher keine Option, den Nutzer selbst ordnungsrechtlich oder gar strafrechtlich zur Verantwortung zu ziehen, wenn er selbstbestimmt ‚unvernünftige', nur sich selbst potentiell gefährdende Angaben in sozialen Netzwerken macht.[1427]

Ähnliches gilt gegenüber den Anbietern sozialer Netzwerke. Zwar könnte diesen auferlegt werden, als riskant eingestuftes Verhalten nicht zu ermöglichen oder ihre Nutzer gar hierzu zu ermutigen. Soweit dies einen Eingriff in die Berufsfreiheit der Anbieter darstellt, ließe sich dieser gegebenenfalls aus der staatlichen Schutzpflicht für die informationelle

[1423] Vgl. für konkrete strafrechtliche Verurteilungen im Zusammenhang mit Facebook beispielsweise OLG Hamm, MMR 2015, 848 (848 f.).
[1424] *Sandfuchs*, Privatheit wider Willen, S. 155 ff.
[1425] So auch *Sandfuchs*, Privatheit wider Willen, S. 166 ff.; *Buchner*, Informationelle Selbstbestimmung, S. 113; vgl. auch *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 91.
[1426] *Sandfuchs*, Privatheit wider Willen, S. 167 f. m.w.N.
[1427] Allgemein für selbstbestimmte Informationspreisgaben so auch *Sandfuchs*, Privatheit wider Willen, S. 168 f.; vgl. auch *Buchner*, Informationelle Selbstbestimmung, S. S. 113 f.

Selbstbestimmung rechtfertigen.[1428] Auch dies würde aber regelmäßig eine überschießende paternalistische Regelung darstellen, die letztlich nur der Erziehung der Nutzer dienen würde. Im Ergebnis macht es insofern keinen Unterschied, ob der Staat Nutzern direkt verbietet, ‚unvernünftige' Angaben in sozialen Netzwerken zu machen oder nur die Anbieter anweist, solche Angaben nicht zu veröffentlichen.

Es wurde bereits darauf hingewiesen, dass auch das Konzept des Datenschutzes durch Technik als paternalistisch angesehen werden kann und sich freiheitseinschränkend gegenüber den Anbietern auswirkt. In diesem Maße ist eine Regulierung der Anbieter sozialer Netzwerke jedoch sinnvoll und auch durch die staatliche Schutzpflicht geboten.[1429] Darüber hinausgehende Beschränkungen, die nicht ohnehin nach allgemeinen Gesetzen bestehen, sind zwar grundsätzlich denkbar; sie müssen aber stets mit ihrer freiheitseinschränkenden Auswirkung abgewogen werden. Die Auswahl derartiger Beschränkungen ist dem politischen, demokratischen Prozess zu überlassen.

[1428] Vgl. *Masing*, NJW 2012, 2305 (2308); ausführlich zu den betroffenen Grundrechten der Anbieter sozialer Netzwerke *Kutscha*, GR-Schutz im Internet, S. 51 ff.

[1429] Zustimmend bezüglich der Schaffung von Rahmenbedingungen zur selbstbestimmten Informationspreisgabe *Sandfuchs*, Privatheit wider Willen, S. 169.

E. Ein Rendezvous mit der Moderne: Das Datenschutzrecht in sozialen Netzwerken des 21. Jahrhunderts

Die global vernetzte, arbeitsteilige und dezentrale Datenverarbeitung, die insbesondere für soziale Netzwerke im Internet prägend ist, bedeutet erhebliche Herausforderungen für das Recht.[1430] Die Analyse in dieser Arbeit hat indes gezeigt, dass das Datenschutzrecht allem Pessimismus zum Trotz sowohl in seiner bisherigen Fassung als auch zukünftig mit der DS-GVO grundsätzlich in der Lage ist, mit diesen Problemen umzugehen. Dennoch wurden die Grenzen des Datenschutzrechts deutlich sichtbar, vor allem mit Blick auf die konkrete Verantwortungszuweisung und die Einwilligung. Daher sollen nun auf konzeptioneller Ebene die Stärken und Schwächen des Datenschutzrechts im Umgang mit diesen Herausforderungen zusammenfassend betrachtet werden. Dabei kristallisiert sich der Charakter des Datenschutzrechts als modernes, rechtsgebietsübergreifendes Risikovorsorgerecht heraus.[1431]

I. Internationalität und Multipolarität als Herausforderungen für die Steuerungskraft des Rechts

Die Globalisierung und die damit verbundene Internationalisierung der Datenverarbeitung führen zu Unklarheiten in der Anwendbarkeit des nationalen Rechts und damit auch der Zuständigkeit staatlicher Durchsetzungsinstanzen. Auf die daraus resultierenden Fragen hat die europäische Union mit der DS-GVO, die mit dem Marktortprinzip sogar einen extraterritorialen Geltungsanspruch erhebt[1432], eine klare Antwort gefunden, um einen hohen und einheitlichen Grundrechtsschutz von Unionsbürgern sicherzustellen. Die staatliche Regulierungsfähigkeit wird hierdurch auch im Angesicht mächtiger, international agierender Datenverarbeitungskonzerne wie Facebook erheblich gestärkt und ein staatliches Regulierungsdefizit, welches vor allem für rein nationale Regelungen drohte[1433], effektiv verhindert.

Als weit größeres Problem erweist sich dagegen die Zuweisung von Verantwortlichkeit innerhalb des anwendbaren Rechts. Das Recht braucht klare Adressaten für seine Regelungen, um durchsetzbar zu sein. Das Datenschutzrecht muss regeln, welche Datenverarbeitung für wen

---

1430 Kritisch zur verbleibenden Steuerungskraft des nationalen Rechts insoweit *Buchholtz*, AöR 2015, 121 (123); *Heckmann*, NJW 2012, 2631 (2632).

1431 Vgl. auch bereits *Spiecker gen. Döhmann*, Verantwortung bei begrenztem Wissen, in: Fehling u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 70 – *Erscheinen in Vorbereitung*; in Bezug auf das europäische Datenschutzrecht auch *Strahilevitz*, 126 Harv. L. Rev. 2010 (2035 f.) 2012-2013.

1432 Hierzu ausführlich oben unter C.I.1.

1433 *Hoffmann-Riem*, AöR 1998, 513 (533); *Buchholtz*, AöR 2015, 121 (144 f.).

erlaubt ist und gegenüber wem Betroffenen gegebenenfalls ihre Rechte geltend machen müssen. In einem natürlichen Konflikt hierzu stehen die zunehmende Arbeitsteilung und die damit einhergehende Verantwortungsdiffusion bei der Erstellung von Datensätzen und Informationen im digitalen Kontext, speziell auch in sozialen Netzwerken.[1434] Das klassische dichotome Verhältnis von einem Datenverarbeiter und dem hiervon Betroffenen hat sich in ein komplexes multipolares Geflecht von Rechtsbeziehungen gewandelt und wirft die Frage auf, wie das Recht hierauf konzeptionell antworten sollte. Als konzeptionelle Alternativen stehen sich hier das bisherige Modell bereichsspezifischer, detaillierter Regelungen mit Zurechnungsmechanismen im Einzelfall und das Modell eines hochabstrakten, „technologieneutralen" Datenschutzrechts gegenüber. Als Ergänzung für beide Modelle steht gegebenenfalls der oben bereits besprochene „Risk-Based Approach" zur Verfügung.[1435] Er bietet einen ersten Ansatz, um auf die sehr unterschiedlichen Verarbeitungskontexte zu reagieren, in denen Daten insbesondere durch Private heute verarbeitet werden, mit teilweise erheblichen Macht- und Informationsgefällen sowohl den Betroffenen als auch sogar dem Staat gegenüber. In jedem Fall kann das Datenschutzrecht die Herausforderungen nicht alleine bewältigen, sondern ist als Querschnittsmaterie auf eine Abstimmung nicht zuletzt mit dem Wettbewerbsrecht, dem Urheberrecht, dem Kartellrecht und dem Verbraucherschutzrecht angewiesen.[1436]

1. Bereichsspezifische, konkrete Regelungen vs. abstrakte Technologieneutralität

a) Der bereichsspezifische Ansatz in der digitalen Realität

Das bisherige deutsche Datenschutzrecht verfolgt einen – wie einst auch vom Bundesverfassungsgericht im Volkszählungsurteil angemahnt[1437] – konkreten, bereichsspezifischen Regelungsansatz. Freilich besteht auch eine gewisse Technologieoffenheit, da nicht zuletzt die spezifischen Begriffe der Datenverarbeitung in § 3 BDSG technologieneutral auszulegen sind.[1438] Zudem sind die gegenwärtig bestehenden Erlaubnistatbestände beispielsweise der §§ 28, 29 ff. BDSG bereits generalklauselartig

[1434] Vgl. *Simo*, Big Data, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung, S. 32; *Spiecker gen. Döhmann*, Verantwortung bei begrenztem Wissen, in: Fehling u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 60 ff. – *Erscheinen in Vorbereitung*; *Hoffmann-Riem*, AöR 2012, 509 (520).
[1435] Oben unter D.III.3.b).
[1436] *Greve*, Drittwirkung, in: FS Kloepfer, S. 668; *Buchner*, Facebook zwischen BDSG und UWG, in: FS Köhler, S. 51 ff.; *Spiecker gen. Döhmann*, K&R 2012, 717 (724 f.).
[1437] BVerfGE 65, 1 (44, 46) – Volkszählung.
[1438] *Dammann*, in: Simits, BDSG, § 3 Rn. 1, 112; *Buchner*, in: Taeger/Gabel, § 3 BDSG, Rn. 25 ff. m.w.N.

ausgestaltet, indem sie eine offene Interessenabwägung zwischen dem Betroffenen und dem Datenverarbeiter ermöglichen.[1439] In seiner Gesamtheit verfolgt das deutsche Datenschutzrecht aber den Ansatz, möglichst klare Vorgaben bezüglich der Rechtmäßigkeit der Datenverarbeitung, der mit dieser verfolgten Zwecke und der daraus jeweils resultierenden Verantwortung zu machen. Dies zeigt sich nicht zuletzt an den zahlreichen unterschiedlichen Erlaubnistatbeständen und Abgrenzungen verschiedener Datenarten sowie -verarbeitungsstadien und Sonderregeln in bereichsspezifischen Gesetzen.[1440] Allen Regelungen liegt das – häufiger kritisierte[1441] – Verbotsprinzip des § 4 BDSG zugrunde, welches eine grundlegende Risikoverteilung für die Rechtmäßigkeit einer Datenverarbeitung zulasten des Datenverarbeiters und zugunsten des Betroffenen vornimmt.[1442]

Im starken Kontrast hierzu steht die Realität des Internets und der ubiquitären Datenverarbeitung, durch welche die traditionellen Grenzen der Medien überschritten werden und sich bereichsspezifische Trennungen auflösen und vermischen.[1443] Soziale Netzwerke mit den durch sie aufgeworfenen Abgrenzungsproblemen[1444] sind hierbei nur ein Beispiel unter vielen. Die Folge ist die Gefahr der übermäßigen „Verrechtlichung“: Eine allzu große Differenzierung schafft widersprüchliche Schutznormen und unüberschaubare bereichsspezifische Pflichten und kreiert damit Glaubwürdigkeitsverluste durch Vollzugsdefizite und rechtliche Intransparenz sowohl für Laien als auch Experten.[1445] Der Vorteil einer bereichsspezifischen Regulierung, eine hohe Rechtssicherheit und demokratische Legitimation der Einzelfallabwägung zu bieten, verkehrt sich damit in sein Gegenteil. Speziell im Datenschutzrecht geht die implizite Stärkung der Grundsätze der Zweckbindung und Datensparsamkeit durch bereichsspezifische Regelung von Erlaubnistatbeständen für Datenverarbeitungen und detaillierte Beschreibung von Verarbeitungsschritten[1446] verloren,

---

[1439] *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 102; *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 55 ff.; *Simitis*, in: Simitis, BDSG, § 28 Rn. 102 ff. m.w.N.

[1440] *Simitis*, in: Simitis, BDSG, § 1 Rn. 23 m.w.N.

[1441] Vgl. beispielsweise *Buchholtz*, AöR 2015, 121 (135); *Heckmann*, NJW 2012, 2631 (2631 f.).

[1442] Vgl. *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 102.

[1443] Ausführlich *Hoffmann-Riem*, AöR 2012, 509 (510 ff.) m.w.N.; vgl. auch *Spiecker gen. Döhmann*, K&R 2012, 717 (725).

[1444] Vgl. beispielsweise die Bestimmung der (international) verantwortlichen Stelle oben unter C.II.4.b), die Zuordnung der unterschiedlichen Datenarten und die Einordnung als Telemedien- oder Telekommunikationsdienst oben unter C.II, die Anwendbarkeit des Haushaltsprivilegs oben unter D.I.3.b)aa) oder die Reichweite der Impressumspflicht oben unter D.II.1.

[1445] Instruktiv bereits *Hoffmann-Riem*, AöR 1998, 513 (514 ff.) m.w.N.; vgl. auch *Buchholtz*, AöR 2015, 121 (134 f.); *Eifert*, Zweckvereinbarkeit, in: *Gropp u.a.* (Hrsg.), S. 140 ff.

[1446] Vgl. hierzu *Nebel/Richter*, ZD 2012, 407 (409 f.).

wenn die Zuordnung des tatsächlichen Sachverhalts zu der rechtlichen Regelung nicht mehr eindeutig *ex ante* erkennbar ist.[1447]

b) Abstrakte Technologieneutralität als Antwort auf zunehmende Komplexität und immer schnelleren technischen Wandel

Als gleichsam heilsbringende Lösung wird zuweilen der Regelungsansatz einer abstrakten Technologieneutralität des Rechts propagiert: Anstatt dem technischen Fortschritt immer hinterherzulaufen, soll das Recht seine Regelungshoheit, Regelungsklarheit und präventive Steuerungswirkung bewahren, indem es einen Abstraktionsgrad erreicht, auf dem es trotz gravierender technischer Änderungen stets anwendbar bleiben kann.[1448] Vom Regelungsanspruch und Schutzumfang des Rechts her gedacht stellt dies keine Neuerung gegenüber dem im Datenschutzrecht seit jeher bestehenden Konsens dar, dass der Schutz personenbezogener Daten nicht von der verwendeten Technik abhängen sollte.[1449] Die geforderte Veränderung liegt vielmehr auf rechtstechnischer Seite, indem bereichsspezifische, detaillierte Regelungen zugunsten von hochabstrakten Generalklauseln aufgegeben werden sollen.[1450] Diese Wünsche wurden weitgehend von der DS-GVO erfüllt, welche in Erwägungsgrund 15 ausdrücklich Technologieneutralität zur Zielvorgabe erklärt und in den sehr allgemein gehaltenen Art. 4 Nr. 2 DS-GVO zu den Verarbeitungsschritten, Art. 4 Nr. 7 DS-GVO für die Bestimmung des Verantwortlichen und Art. 6 DS-GVO mit seinen nicht bereichsspezifischen Erlaubnistatbeständen umsetzt.

Diese idealisierte Betrachtung der Technologieneutralität übergeht freilich den erheblichen Konkretisierungsbedarf, den übermäßig abstrakte Regelungen aufweisen, sofern sie – wie dies insbesondere das Ziel des europäischen Datenschutzrechts ist – einheitlich angewandt werden sollen.[1451] Recht, das nach seinem abstrakten Wortlaut nahezu jede Fallgestaltung regeln könnte, regelt schlussendlich keine Einzige. Insofern bedeutet eine derart umgesetzte

---

[1447] Kritisch gegenüber der bereichsspezifischen Regelung deshalb *Buchholtz*, AöR 2015, 121 (134 f.); ausführlich hierzu *Kühling*, Die Verwaltung (44) 2011, 523 (553 ff.).

[1448] *Buchholtz*, AöR 2015, 121 (144 ff.); vgl. auch *Bull*, NVwZ 2011, 257 (259).

[1449] Dieser Grundsatz war beispielsweise bereits in Erwägungsgrund 27 DSRL enthalten und folgt auch aus dem Gebot eines effektiven Grundrechtsschutzes. Er war trotz der bereichsspezifischen Regelungen im deutschen Datenschutzrecht stets zu beachten, indem beispielsweise die detailliert normierten Formen der Datenverarbeitung in § 3 BDSG technikneutral auszulegen waren, vgl. statt vieler *Dammann*, in: Simitis, BDSG, § 3 Rn. 1, 112. Der Grundsatz der Technik- oder Technologieneutralität stellt somit keinesfalls eine vollständige konzeptionelle Neuerung der DS-GVO dar.

[1450] So etwa *Buchholtz*, AöR 2015, 121 (134 ff., 144 ff.).

[1451] *Roßnagel/Kroschwald*, ZD 2014, 495 (497); *Sydow/Kring*, ZD 2014, 271 (272 f.); *Roßnagel/Richter/Nebel*, ZD 2013, 103 (104 ff.); vgl. auch *Kühling*, Die Verwaltung (44) 2011, 523 (552 f.); *Ders./Martini*, EuZW 2016, 448 (449).

Technologieneutralität die Verweigerung der Abwägung und Entscheidung von Interessenkonflikten durch den demokratisch legitimierten Gesetzgeber und eine Delegierung dieser Verantwortung an die Judikative oder Exekutive. Derartige Interessenkonflikte sind aber gerade im Datenschutzrecht als rechtsgebietsübergreifender Querschnittsmaterie, die in zahlreichen Lebens- und Wirtschaftssituationen von Bedeutung ist,[1452] sehr verbreitet und werden durch eine Weiterentwicklung der technischen Möglichkeiten eher zu- als abnehmen. Ein Datenschutzrecht, das sich der Auseinandersetzung mit und Lösung von diesen Interessenkonflikten verweigert und nur hochabstrakte, allgemeine Leitlinien in Form von Generalklauseln aufstellt, entzieht sich seiner Verantwortung und entkoppelt sich von der Realität, die es mit diesem Ansatz endgültig einzufangen versucht. Der vermeintliche Gewinn in der Steuerungsfähigkeit des Rechts wird durch einen Verlust an Rechtssicherheit und demokratischer Legitimation erkauft.[1453]

Bäcker weist zwar darauf hin, dass die staatliche Schutzpflicht gegenüber privater Datenverarbeitung zu weniger hohen Anforderungen an die Regelungsdichte des einfachen Rechts führt als dies bei einem Abwehrrecht der Fall wäre: Anstatt „jede denkbare punktuelle Gefährdung des Einzelnen durch private Informationshandlungen eigenhändig zu normieren", könne grundsätzlich auf Generalklauseln zurückgegriffen werden, welche durch die Rechtsprechung konkretisiert werden.[1454] Dem ist insoweit zuzustimmen, als eine Einzelfallregelung durch den Gesetzgeber tatsächlich mangels der Vielzahl an denkbaren Fallkonstellationen und unterschiedlichen Interessenlagen unmöglich ist. Anders als für staatliche Datenverarbeitung sind für private Datenvearbeitungen mangels eines direkten Grundrechtseingriffs auch keine gesetzlichen Ermächtigungsnormen erforderlich.[1455] Dennoch lassen sich derartige Generalklauseln unterschiedlich konkret ausgestalten; wie nicht zuletzt die §§ 28, 29 BDSG zeigen, steht ein bereichsspezifischer, konkreter Regelungsansatz keineswegs in einem Widerspruch zu einer wohlüberlegten Verwendung von Generalklauseln.[1456]

[1452] Vgl. *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 125; *Greve*, Drittwirkung, in: FS Kloepfer, S. 667; *Buchner*, Facebook zwischen BDSG und UWG, in: FS Köhler, S. 55 ff.; *Spiecker gen. Döhmann*, K&R 2012, 717 (724 f.).

[1453] Dies übergeht *Buchholtz*, AöR 2015, 121 (135, 144 ff.) in ihrem Plädoyer für eine Entwicklung eines „internetgerechten Kriterienkatalogs" für die „Voraussetzungen des freien Entscheidens im Internet" durch die Rechtsprechung und einer damit einhergehenden Abstraktion des Rechts in Form datenschutzrechtlicher Generalklauseln.

[1454] *Bäcker*, Der Staat (51) 2012, 91 (99 f.); vgl. zum Untermaßverbot *Greve*, Drittwirkung, in: FS Kloepfer, S. 674 f.

[1455] *Bäcker*, Der Staat (51) 2012, 91 (100).

[1456] Vgl. *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 36, 102; *Roßnagel/Richter/Nebel*, ZD 2013, 103 (104).

c) Der Preis hochabstrakter Regelungen

Ein hochabstraktes Datenschutzrecht schadet vornehmlich den Interessen und Schutzgütern, die es schützen sollte. Das unter anderem in den Erwägungsgründen 7, 9 und 13 DS-GVO ausgedrückte Ziel der Vereinheitlichung des Datenschutzes zur Förderung von Wirtschaftsinteressen und insbesondere von kleinen und mittleren mittelständischen Unternehmen droht durch einen uneinheitlichen Vollzug konterkariert zu werden.[1457] Unklare Regelungen präsentieren wirtschaftliche Risiken für solche Unternehmen, weil keine abschließenden Auskünfte beispielsweise über notwendige Sicherheitsmaßnahmen oder auch nur die Voraussetzungen für die Rechtmäßigkeit einer Datenverarbeitung gegeben werden können. Gleichzeitig sind auch der Schutz personenbezogener Daten Betroffener und die hierhinter stehenden Grundrechte bedroht, da stark konkretisierungsbedürftige Regelungen langwierige Gerichtsverfahren bis vor den EuGH geradezu herausfordern. Dies erzeugt lange Phasen der Rechtsunsicherheit, in welcher Betroffene gegebenenfalls unzulässigen Datenverarbeitungspraktiken ausgesetzt sind, ohne ihre Rechte effektiv durchsetzen zu können.[1458] Große Datenverarbeitungsunternehmen wie Facebook oder Google werden hingegen nicht nennenswert negativ beeinflusst, da sie sich einerseits gute Rechtsanwälte leisten und andererseits lange Gerichtsverfahren aussitzen und im Falle eines verlorenen Prozesses gegebenenfalls Schadensersatzsummen zahlen, bis dahin aber ihre Praktiken fortsetzen und somit sogar von der Rechtsunsicherheit profitieren können.[1459] Gleichzeitig prägen solche großen Telekommunikations- und Telemediendienstleister die Realität und Praxis im Internet in ihrem Sinne und schaffen hierdurch Fakten, die die staatliche Schutzpflicht unterlaufen könnten.[1460]

Ein übermäßig technologieneutrales, abstraktes Datenschutzrecht verfehlt somit zwingend sein Ziel der Rechtsklarheit und Rechtssicherheit.[1461] Es stellt keine angemessene Lösung für die

[1457] Vgl. *Sydow/Kring*, ZD 2014, 271 (272); *Klar*, DÖV 2013, 103 (111 f.); *Roßnagel/Nebel/Richter*, ZD 2015, 455 (457); *Roßnagel*, in: Ders. (Hrsg.), Europäische DS-GVO, § 1 Rn. 36 ff.; instruktiv zur Notwendigkeit einer (Teil-)Verrechtlichung von informellem Verwaltungshandeln und den Gefahren maximaler Verfahrensflexibilität *Fehling*, Informelles Verwaltungshandeln, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II, § 38 Rn. 83 ff., 99 ff.

[1458] Vgl. *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 102; *Spiecker gen. Döhmann*, K&R 2012, 717 (725).

[1459] In Abwesenheit eines Verbandsklagerechts werden derartige Durchsetzungsdefizite dadurch weiter verstärkt, dass viele Private darauf verzichten, ihre Interessen vor Gericht durchzusetzen, gerade auch in Datenschutzfragen, vgl. *Mayer-Schönberger*, Die Tugend des Vergessens, S. 165 f.

[1460] Vgl. *Greve*, Drittwirkung, in: FS Koehler, S. 677; *Lessig*, Code is Law, http://www.harvardmagazine.com/2000/01/code-is-law-html.

[1461] Vgl. *Simitis*, in: Simitis, BDSG, § 1 Rn. 107; *Roßnagel*, in: Ders. (Hrsg.), Europäische DS-GVO, § 1 Rn. 29 ff.

Probleme von politisch trägen Entscheidungsprozessen und einem hieraus resultierenden veralteten bereichsspezifischen Datenschutzrecht dar. Der Gewinn eines hochabstrakten, technologieneutralen Rechts liegt wenn überhaupt, dann nur auf dogmatisch-theoretischer Ebene, auf welcher es stets an neue Gegebenheiten angepasst werden kann, ohne dass logische Brüche auftreten. Auf dieser Ebene ist das Recht indes selbstreferentiell und bar jeglicher praktischer Relevanz. Das Recht gewinnt seine praktische Bedeutung dadurch, dass es Lebenssachverhalte regelt und Interessenkonflikte verbindlich entscheidet. Hierfür muss es zu einem gewissen Grad konkret werden und damit das Risiko eingehen zu veralten, wenn sich die Lebenssachverhalte deutlich wandeln.[1462] Wer das Problem unklarer Normen und Abgrenzungsfragen unter neuen technologischen Bedingungen lösen will, indem er diese Klarheit für alle Sachverhalte abschafft und auf eine kasuistische Klärung im Einzelfall verweist, erweist der Rechtssicherheit offensichtlich einen Bärendienst.

Im Angesicht des rasanten technologischen Fortschritts und der ubiquitären, globalen Datenverarbeitung mag die Forderung nach einem detaillierten, konkreten und doch flexiblen Datenschutzrecht zunächst anmaßend und nachgerade unerfüllbar anmuten. Es soll hier auch keinesfalls verkannt werden, dass die Herausforderungen einer Regulierung angesichts der unterschiedlichen globalen Akteure, grenzüberschreitendem Wirken und rasanter technologischer Innovation erheblich wären.[1463] Sich dieser Herausforderung zu stellen und sie nicht defätistisch abzutun, ist indes eine notwendige Voraussetzung, um trotz der zunehmenden technologischen Komplexität, der Globalisierung, der zunehmenden Verantwortlichkeitsdiffusion durch Technik und Arbeitsteilung und der Abstraktion von politischen Entscheidungsebenen weg vom mündigen Bürger vor Ort in einem demokratisch organisierten und regulierten Gemeinwesen zu leben. Das Datenschutzrecht berührt als Querschnittsmaterie infolge der ubiquitären Datenverarbeitung heutzutage nahezu sämtliche Lebensbereiche und erlangt damit eine besondere gesellschaftliche Relevanz. Ein Rückzug der Politik aus diesem Bereich und die weitgehende, wenn nicht gar vollständige Überantwortung

[1462] So auch *Sydow/Kring*, ZD 2014, 271 (272 f.); *Spiecker gen. Döhmann*, K&R 2012, 717 (725).
[1463] Ausführlich und differenziert hierzu *Hoffmann-Riem*, AöR 2012, 509 (516 ff., 533 ff.).

des Interessenausgleichs an die Exekutive und Judikative sowie an private Rechtssetzung[1464] kommt einer Bankrotterklärung demokratischer Entscheidungsprozesse im Rahmen der Regulierung digitaler Datenverarbeitung gleich.[1465]

Ein modernes Datenschutzrecht, das sich nicht solcher Beliebigkeit anheimgeben will, muss sich daher auf die Herausforderung und das Risiko einlassen, technische Fragen nicht nur mit hochabstrakten Generalklauseln nach dem Schema „one size fits all" abzutun, sondern detailliertere und soweit notwendig auch bereichsspezifische Regelungen zu treffen.[1466] Die real auftretenden Konflikte werden nicht dadurch einfacher, dass sie mit schlichteren Regeln entschieden werden sollen. Es ist die Bürde demokratischer Gesetzgebung, sich hiermit zu befassen und einen Kompromiss zwischen der konkreten Regulierung aktuell bekannter Interessenkonflikte und zukünftiger, derzeit noch nicht konkret absehbarer Entwicklungen zu finden.[1467]

[1464] Freilich geht es hierbei um eine Frage der Schwerpunktsetzung. Bereits im Status Quo wird ein erheblicher Teil der Funktionsweise des Internets – speziell auch sozialer Netzwerke – durch Regeln bestimmt, die von Privaten gesetzt wurden. Selbstregulierungskonzepte und nichtstaatliche Akteure, allen voran die ICANN als für die Domainvergabe zuständige Institution, prägen nicht zuletzt den Aufbau des Internets und den Umgang seiner Nutzer untereinander. Hinzu kommen faktische Regeln, die durch Voreinstellungen und Programmierungen erzeugt werden. Derartige private Rechtssetzung bereichert das Internet und fängt staatliche Regulierungsdefizite auf. Sich mit ihnen zu begnügen und den Staat daher aus der Verantwortung zu entlassen, verkennt aber, dass solche privaten Regeln nicht aus einer gemeinwohl- und rechtsgüterschutzorientierten Perspektive gesetzt werden, sondern auf die bloße Funktionsfähigkeit des Internets und seiner Dienste ausgerichtet sind. Gerade im Fall kommerzieller Akteure wie Google, Facebook oder Amazon stehen zudem rein egoistische Gewinninteressen im Vordergrund. Die Entwicklung der letzten Jahre hat gezeigt, dass solche kommerziellen Akteure durch Bildung von Oligopolen in kurzer Zeit unverhältnismäßig viel Macht erhalten können. Angesichts der enormen Bedeutung des Internets als öffentlichem Raum sollte der Staat daher als demokratische, gemeinwohlorientierte Instanz zumindest klare Rahmenbedingungen setzen, innerhalb derer private Rechtssetzung stattfinden kann; so zum hier Beschriebenen bereits ausführlich *Hoffmann-Riem*, AöR 2012, 509 (531 ff.); vgl. zu den Grenzen privater Selbstregulierung im digitalen Kontext auch *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 103 f.; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 153 ff.

[1465] Insbesondere im US-amerikanischen Diskurs wird dieses grundsätzliche Problem der (vermeintlich) abnehmenden Steuerungskraft des Rechts vor allem aus einer rechtsökonomischen Perspekive diskutiert, vgl. den instruktiven Überblick bei *Mayer-Schönberger*, Informationsrecht als Gestaltungsaufgabe, in: FS Druey, S. 856 ff. m. zahlreichen w.N. Doch auch diese eher defätistische oder jedenfalls pessimistische Haltung gegenüber der Steuerungskraft des Rechts, die beispielsweise in *Lessigs* Analyse „Code is Law" (http://www.harvardmagazine.com/2000/01/code-is-law-html) durchscheint, ist letztlich geprägt von dem Bestreben, diese Steuerungskraft wiederherzustellen. Es wäre daher höchst widersinnig, wenn ausgerechnet Europa, mit seinem insgesamt deutlich höheren Datenschutzniveau, nun dauerhaft den Weg der weitgehenden Selbstaufgabe des legislativen Datenschutzes einschlüge. Vgl. rechtsvergleichend zum Datenschutzniveau in Europa und den USA instruktiv *Sandfuchs*, Privatheit wider Willen, S. 70 ff., 92 ff.; *Fehling*, Privacy, in: ders. u.a. (Hrsg.), Macht und Verantwortungsstrukturen, S. 122 ff. – *Erscheinen in Vorbereitung*.

[1466] Vgl. auch *Simitis*, in: Simitis, BDSG, § 1 Rn. 107 ff.

[1467] Vgl. auch bereits *Sydow/Kring*, ZD 2014, 271 (272 f.); *Roßnagel/Richter/Nebel*, ZD 2013, 103 (104); *Simitis*, in: Simitis, BDSG, § 1 Rn. 23; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 153 ff.

2. Die Steuerungsfähigkeit des Datenschutzrechts im Kontext sozialer Netzwerke

Die in dieser Arbeit aufgeworfenen datennschutzrechtlichen Fragen sozialer Netzwerke konnten im Rahmen des bisherigen und auch des zukünftig geltenden Rechts geklärt werden. Das aktuelle Datenschutzrecht hält daher grundsätzlich Antworten auf die neuen Herausforderungen bereit. Kollisionsrechtlich ist durch die Zugrundelegung des wirtschaftlich-funktionellen Verantwortlichkeitsbegriffs die Anwendbarkeit europäischen – und ggf. sogar deutschen – Datenschutzrechts gegenüber Anbietern sozialer Netzwerke mit Sitz inner- und außerhalb der europäischen Union sichergestellt, so dass eine grundsätzliche Steuerungsmöglichkeit besteht. Den einzelnen Akteuren in sozialen Netzwerken können trotz der teilweise arbeitsteiligen Datenverarbeitung klare datenschutzrechtliche Verantwortlichkeiten zugewiesen werden. Entsprechend sind gegenwärtig und auch zukünftig zumindest die rechtlichen Voraussetzungen dafür gegeben, einen wirksamen Schutz insbesondere der informationellen Selbstbestimmung von Unionsbürgern in sozialen Netzwerken sicherzustellen.[1468]

Die Arbeit hat indes auch die Grenzen der rechtlichen Steuerung in sozialen Netzwerken aufgezeigt: Zunächst erfordert die Zuweisung von Verantwortlichkeit teilweise komplexe Rückgriffe auf allgemeine Grundsätze des Ordnungsrechts oder sich aus der Lektüre des Art. 4 Nr. 7 DS-GVO jedenfalls nicht unmittelbar und klar ergebende Abwägungsergebnisse. Obwohl das Problem damit grundsätzlich rechtlich handhabbar ist, stellt es doch eine mögliche Quelle für erhebliche Rechtsunsicherheit in der Praxis dar.

Vor allem die effektive Sicherung der positiven informationellen Selbstbestimmung und ein Ausgleich der in sozialen Netzwerken bestehenden Informations- und Machtgefälle erweist sich als bisher weitgehend ungelöstes praktisches Problem. Zentral ist hierbei die – sogleich unter E.II. noch einmal gesondert zu diskutierende – Rolle der datenschutzrechtlichen Einwilligung und ihre Flankierung durch staatliche Maßnahmen. Auch bei diesen Problemen besteht aber immerhin eine abstrakte Steuerungsfähigkeit des Rechts, auch wenn diese im Detail noch stärker realisiert werden sollte: Wie oben unter D.III.3. gezeigt wurde, stellen die Stärkung des Selbstdatenschutzes und – soweit sie denn praktisch umsetzbar sind[1469] – an das

[1468] Auch für das Datenschutzrecht in sozialen Netzwerken gilt somit, dass nicht die Steuerungsfähigkeit des Rechts an sich in Frage steht, sondern lediglich das Ausmaß, in welchem das Recht dem heutigen Bedürfnis nach passgenauer und damit komplexerer Steuerung in speziellen Bereichen nachkommen kann, vgl. instruktiv auf abstrakter steuerungstheoretischer Ebene *Fehling*, Informelles Verwaltungshandeln, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II, § 38 Rn. 45 ff.

[1469] Vgl. oben unter D.III.3.b).

konkrete Risiko angepasste datenschutzrechtliche Regelungen erfolgsversprechende Regulierungsansätze dar. Auch die hohen Bußgelder der DS-GVO können durch den Abschreckungseffekt[1470] das staatliche Informationsdefizit zwar nicht beheben, aber dennoch auf eine stärkere Beachtung der datenschutzrechtlichen Regelungen hoffen lassen. Die effektive Regulierung sozialer Netzwerke wird zudem in dem Maße noch besser gelingen, wie die Rechtspraxis auf die Realität des Datenschutzrechts als Querschnittsmaterie reagiert und seine zahlreichen Berührungspunkte und Überschneidungen mit dem Verbraucherschutzrecht, dem Wettbewerbsrecht, dem Kartellrecht und dem allgemeinen Medien- und Vertragsrecht erkennt und aktiv nutzt.[1471] Es wäre verfehlt, vom Datenschutzrecht zu erwarten, die mit diesen anderen Rechtsgebieten verknüpften Probleme eigenständig zu lösen.[1472]

Eine der größten Herausforderungen auf Ebene der Normsetzung besteht darin, einen Ausgleich in dem zuvor aufgezeigten Spannungsfeld von konkreten bereichtsspezifischen Regelungen und einer Flexibilität gegenüber technischen Neuerungen zu finden. Die DS-GVO in ihrer nunmehr verabschiedeten Form stellt hierbei angesichts der zahlreichen hochabstrakten Regelungen mitnichten ein optimales Ergebnis dar. Sie bedarf dringend weiterer Konkretisierung, um vorhersehbar und eindeutig anwendbar und vollziehbar zu sein und damit eine effektive rechtliche Steuerung zu gewährleisten. Wie in dieser Arbeit herausgearbeitet wurde, kann hierbei jedenfalls indiziell auf Fallgruppen zurückgegriffen werden, die nach dem konkreteren bisherigen nationalen Datenschutzrecht gebildet wurden, soweit dieses auf der europäischen Datenschutzrichtlinie beruhte.

Trotz aller Schwierigkeiten besteht somit insofern Grund zum Optimismus, als soziale Netzwerke sich grundsätzlich als datenschutzrechtrechtlich handhabbar erweisen.[1473]

[1470] Art. 83 Abs. 4 DS-GVO bestimmt Geldbußen bis zu 10 Mio. Euro bzw. 2% des Jahresumsatzes des Unternehmens, Art. 83 Abs. 5 DS-GVO verdoppelt diese Höchstgrenzen für bestimmte Verstöße; instruktiv hierzu *Dieterich*, ZD 2016, 260 (264 f.); kritisch zur Vermischung des datenschutzrechtlichen und kartellrechtlichen Unternehmensbegriffs bei der Bestimmung des maßgeblichen Jahresumsatzes *Faust/Spittka/Wybitul*, ZD 2016, 120 (123 f.).

[1471] Vgl. zum Datenschutzrecht als Querschnittsmaterie *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, S. 125.

[1472] Ausführlich zum Zusammenspiel unterschiedlicher Rechtsgebiete zur Regulierung der Internetökonomie *Hoffmann-Riem*, Innovation und Recht, S.651 ff.

[1473] Auf einem anderen Blatt steht freilich, ob diese grundsätzliche Möglichkeit der rechtlichen Regulierung auch durch effektive Rechtsdurchsetzung verwirklicht wird, vgl. hierzu kritisch *Hoffmann-Riem*, Innovation und Recht, S. 655 f.

II. Zwischen Freiheitsermöglichung und Freiheitseinschränkung: Die Einwilligung und die Risikovorsorge

Die Einwilligung steht im Kontext sozialer Netzwerke. aber auch allgemein bei moderner Datenverarbeitung vor einem Dilemma: Auf der einen Seite ist sie ein elementarer Bestandteil einer eigenverantwortlichen, selbstbestimmten Informationspreisgabe. Die vollständige Abschaffung der Einwilligung und Ersetzung durch streng paternalistische Regelungen, die die Zulässigkeit individueller Datenpreisgabe und Datenverarbeitung abschließend regeln, würden daher einen nicht zu rechtfertigenden Eingriff in die individuelle Selbstbestimmung bedeuten.[1474] Auf der anderen Seite sind die Konsequenzen einer Datenverarbeitung im digitalen Kontext, gerade in Verbindung mit Big Data Anwendungen, oft derart kompliziert, dass die bloße Möglichkeit einer wahrhaft informierten Einwilligung bereits in Frage steht. Erschwerend kommen soziale Zwänge hinzu, die Zweifel an der Freiwilligkeit vieler Einwilligungen wecken.[1475] Die Einwilligung ist somit einerseits unverzichtbar, scheint aber andererseits nicht realisierbar. Der Regulierungsauftrag an das Recht ist daher klar: Es müssen Rahmenbedingungen geschaffen werden, die eine individuelle, selbstbestimmte Preisgabe und Verwaltung von Informationen ermöglichen; problematisch ist die praktische Umsetzung dieses Auftrags. Orientierung können Regelungen aus dem Verbraucherschutzrecht, aber auch dem Wettbewerbsrecht und dem allgemeinen Risikovorsorgerecht bieten.

Der schutzwürdige, einem Informations- und Machtgefälle ausgesetzte Nutzer ist mitnichten ein exklusives Phänomen des Datenschutzrechts; auch in anderen privatrechtlichen Gestaltungen kann es zu einem solchen Schutzbedürfnis kommen. Dies ist eine der grundlegenden Erkenntnisse und Annahmen des allgemeinen Verbraucherschutzrechts.[1476] Insofern ist *Buchner* beizupflichten, wenn er schreibt, dass das bestehende Informations- und Machtgefälle für sich genommen noch kein Anlass ist, „von der Maxime der Privatautonomie im Datenschutzrecht Abstand zu nehmen“[1477]. Wie bereits festgestellt wurde, ist die Wahrung

---

[1474] Ausführlich *Sandfuchs*, Privatheit wider Willen, S. 125 ff. m.w.N.; *Rogosch*, Die Einwilligung im Datenschutzrecht, S. 106 f.; vgl. auch bereits oben unter D.III.4.a).

[1475] *Spiecker gen. Döhmann*, K&R 2012, 717 (720 f.); *Grimmelmann*, 94 Iowa L.Rev. 1137 (1181 ff.), 2008-2009; ausführlich zu Defiziten der Einwilligung im Kontext sozialer Netzwerke oben unter D.III.2; vgl. auch ausführlich zur Einwilligung und ihren Defiziten in digitalen Kontexten *Radlanski*, Das Konzept der Einwilligung, S. 19 ff., 192 ff. und *Rogosch*, Die Einwilligung im Datenschutzrecht, S. 106 ff., jeweils m.w.N.

[1476] *Buchner*, Informationelle Selbstbestimmung, S. 109 f.; instruktiv zu den Hintergründen des Verbraucherschutzrecht *Michlitz/Purnhagen*, in: MüKo-BGB, Bd. 1, Vor §§ 13, 14 BGB, Rn. 3 ff.

[1477] *Buchner*, Informationelle Selbstbestimmung, S. 109.

der informationellen Selbstbestimmung der Betroffenen nicht dadurch zu erreichen, dass sie vollständig durch eine staatliche Bevormundung ersetzt und fingiert wird.[1478]

Ebenso erscheint es aber utopisch, jedenfalls im Bereich der hier analysierten sozialen Netzwerke, dass sich die informationelle Selbstbestimmung durch eine weitgehend privatautonome Gestaltung sicherstellen lässt.[1479] Es mutet zwar zunächst wie eine optimale, freiheitsmaximierende Lösung an, die Betroffenen eigenverantwortlich über die Zulässigkeit und Grenzen privater Datenverarbeitung entscheiden zu lassen und die Bedeutung der Einwilligung gegenüber gesetzlichen Erlaubnistatbeständen hierfür sogar noch auszudehnen, um der Vielzahl an möglichen Fallkonstellationen bestmöglich zu begegnen.[1480] Diese Lösung scheitert indes sowohl am faktisch feststellbaren Desinteresse zahlreicher Betroffener an den Konsequenzen der Verarbeitung ihrer Daten[1481] (hierzu sogleich unter 1.) als auch an einem klassischen Marktversagen im Hinblick auf die Korrektur von Datenschutzverstößen[1482] (hierzu anschließend unter 2.).

1. Desinteresse, Überforderung und erlaubtes Risiko

Die datenschutzrechtliche Einwilligung weist neben den herausgearbeiteten konzeptionellen Schwächen[1483] einen grundsätzlichen Unterschied zum allgemeinen Verbraucherschutzrecht auf: Als Teil der positiven informationellen Selbstbestimmung ist es einem Betroffenen möglich, auch zu seinem eigenen Nachteil von geltenden Schutzvorschriften abzuweichen und in für ihn objektiv ungünstige Datenverarbeitungen einzuwilligen. Im allgemeinen Verbraucherschutzrecht wird diese Möglichkeit häufig nicht gewährt, beispielsweise erklärt § 475 BGB für Verbraucher nachteilige Abweichungen von gesetzlichen Schutzregeln unter anderem bei der Verjährung oder Mängelgewährleistung für unwirksam und macht es Verbrauchern damit unmöglich, effektiv in solche einzuwilligen.[1484] Dem liegt nicht zuletzt der grundsätzliche Gedanke des Verbraucherschutzrechts zugrunde, ein möglicherweise

[1478] Oben unter D.III.4.a); vgl. auch *Buchner*, Informationelle Selbstbestimmung, S. 113 f.; *Radlanski*, Das Konzept der Einwilligung, S. 220 f.

[1479] Zur privatautonomen Gestaltung des Datenschutzrechts ausführlich *Buchner*, Informationelle Selbstbestimmung, S. 118 ff., der konsequenterweise auch für eine Einstufung des Rechts auf informationelle Selbstbestimmung als Vermögensrecht plädiert, vgl. a.a.O. S. 208 ff.

[1480] Ausführlich *Buchner*, Informationelle Selbstbestimmung, S.118 ff., 130 f.

[1481] So auch *Radlanski*, Das Konzept der Einwilligung, S. 222 f.; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 240 ff.

[1482] Vgl. hierzu *Hermstrüwer*, Informationelle Selbstgefährdung, S. 134 ff.

[1483] Vgl. hierzu bereits oben unter D.III.2.

[1484] Vgl. *Lorenz*, in: MüKo-BGB, Bd. 3, § 475 BGB, Rn. 1 f., 9; vgl. auch *Radlanski*, Das Konzept der Einwilligung, S. 222 f.

bestehendes Macht- und Informationsgefälle auszugleichen und zu verhindern, dass der Unternehmer den Verbraucher zum Verzicht auf entsprechende Rechte drängt.[1485]

Ferner zeigen die Regelungen der §§ 305 ff. BGB, dass sich der Gesetzgeber durchaus bewusst ist, dass die bloße Bereitstellung von Informationen keinesfalls zwingend ein Verständnis dieser Informationen bedingt. Entsprechend ist es nur folgerichtig, dass überraschende Klauseln in AGB gemäß § 305c BGB nicht Bestandteil eines Vertrages werden und die §§ 307 ff. BGB eine unangemessene Benachteiligung von Vertragspartnern, insbesondere von Verbrauchern, für unwirksam erklären. Es belegt die gesetzgeberische Annahme, dass Vertragspartner im Allgemeinen und Verbraucher im Besonderen AGB im Regelfall weder detailliert lesen noch dass sie dies tun sollten.[1486] Angesichts des ökonomischen Schadens, der mit dem ausführlichen Lesen in Form von Opportunitätskosten verbunden wäre, ist dies nur konsequent.[1487]

Es gibt keinen empirischen Grund zu der Annahme, dass Betroffene einer möglichen Datenverarbeitung den Datenrichtlinien kritischer und aufmerksamer entgegentreten als sie dies bei klassischen AGB tun würden. Eine ehrliche Diskussion über die Möglichkeiten der Einwilligung bei der Sicherung der informationellen Selbstbestimmung im Kontext sozialer Netzwerke, aber auch darüber hinaus, muss diese Realität anerkennen.[1488]

Radlanski diskutiert in seiner kürzlich erschienenen Dissertation – unter Berücksichtigung der bisher hierzu erschienenen umfangreichen Literatur – verschiedene Lösungsansätze, um dieser Überforderung der Betroffenen zu begegnen und eine größere Effektivität der Einwilligung, insbesondere ihrer Freiwilligkeit zu gewährleisten. Die vorgeschlagenen Lösungen umfassen unter anderem eine Abstimmung von Einwilligungsklauseln mit Aufsichtsbehörden, verpflichtende Opt-In-Regelungen und zeitliche Beschränkungen.[1489] Seinem Ergebnis, dass letztlich keine dieser Lösungen geeignet ist, eine Freiwilligkeit der Einwilligung angesichts der

---

[1485] Der Verbraucherschutz wird weiter durch das in § 475 Abs. 1 S. 2 BGB ausdrücklich normierte und für europarechtlich geprägte Verbraucherschutzgesetze typische Umgehungsverbot gestärkt, vgl. *Lorenz*, in: MüKo-BGB, Bd. 3, § 475 BGB, Rn. 28 ff.; vgl. allgemein zur typisierten Schutzbedürftigkeit von Verbrauchern *Micklitz/Purnhagen*, in: MüKo-BGB, Bd. 1, § 13 BGB, Rn. 3 ff.

[1486] So auch bereits *Radlanski*, Das Konzept der Einwilligung, S. 223.

[1487] *Grimmelmann*, 94 Iowa L.Rev. 1137 (1182), 2008-2009 m.w.N.

[1488] Vgl. *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 104 ff.; *Bäcker*, Der Staat (51) 2012, 91 (112 f.) bezeichnet das „Leitbild des aufkmerksamen Betroffenen" als „weitghend illusorisch"; *Radlanski*, Das Konzept der Einwilligung, S. 222 f., spricht insoweit von einem notwendigen Abschied vom „Traumbild des mündigen Betroffenen"; vgl. aus rechtsökonomischer Perspektive *Fehling*, Evolving Law and Economics of Internet Privacy, in: Eger u.a. (Hrsg.), Economic Analysis of International Law, S. 104.

[1489] *Radlanski*, Das Konzept der Einwilligung, S.212 ff., 215; eine ähnliche Richtung schlagen auch die von *Hermstrüwer*, Informationelle Selbstgefährdung, S. 366 ff., 373 ff. unterbreiteten Vorschläge ein.

Informationsdefizite und dem strukturellen Desinteresse vieler Betroffener sicherzustellen[1490], ist zuzustimmen. Seine Schlussfolgerung, den Anwendungsbereich der Einwilligung erheblich einzuschränken und ihre Wirksamkeit insbesondere von einem Nachweis abhängig zu machen, dass die Einwilligung im objektiven Interesse des Betroffenen liegt[1491], bleibt indes die Antwort schuldig, wie dieses objektive Interesse letztlich bestimmt und subsumiert werden soll. Angesichts der enormen Vielfältigkeit von Konstellationen, in denen es aus den unterschiedlichsten Interessen heraus zu einer Datenverarbeitung kommen kann, scheint es unmöglich, hier auf abstrakt-genereller Ebene klare Fallgruppen zu bilden.[1492] Ohne diese Antwort bietet der Ansatz aber kaum einen Gewinn an Rechtssicherheit gegenüber der bisherigen Bestimmung der Einwilligung, bei welcher es auf die Subsumtion des diffusen Begriffs der Freiwilligkeit ankommt. Im schlimmsten Fall bedeutet er dagegen eine massive Beschränkung in Form einer de facto Abschaffung der individuellen Einwilligung in vielen Bereichen.

Wenn an der positiven informationellen Selbstbestimmung als Recht auf selbstbestimmte Datenpreisgabe festgehalten werden soll, gibt es daher keine einfachen Antworten. Der Staat steht in der Schutzpflicht, durch eine Stärkung des Selbstdatenschutzes, des Datenschutzes durch Technik und vermehrte Aufklärung der Betroffenen Informations- und Rationalitätsdefizite abzubauen und zu kompensieren.[1493] Realistischerweise wird dies aber jedenfalls bei einer signifikanten Anzahl der Betroffenen nicht dazu führen, dass diese Defizite vollständig verschwinden. Letztendlich stellt sich somit die Grundsatzfrage, ob dieses Risiko einer gleichsamen Selbstentmündigung der Betroffenen von der Gesellschaft und vom Recht toleriert werden sollte. Angesichts der Tatsache, dass die einzige bisher gefundene und plausible Alternative eine noch viel weitergehende Entmündigung aller Betroffenen ist, indem ihnen die Möglichkeit zu einer selbstbestimmten Einwilligung gänzlich qua Gesetz genommen wird, scheint es recht eindeutig, dass diese Entscheidung nur zugunsten des tolerierten Risikos ausgehen kann. Auch hier zeigt sich somit deutlich der Charakter des Datenschutzrechts als Risiko*vorsorge*-, aber nicht Risikoausschließungsrecht.[1494]

[1490] *Radlanski*, Das Konzept der Einwilligung, S. 221 ff., 232 ff.; in diese Richtung auch bereits *Rogosch*, Die Einwilligung im Datenschutzrecht, S. 80 ff. m.w.N.

[1491] *Radlanski*, Das Konzept der Einwilligung, S. 232 f.

[1492] *Buchner*, Informationelle Selbstbestimmung, S. 110 ff.

[1493] Zu diesen Maßnahmen bereits ausführlich oben unter D.III.3.a). Dies betont auch *Hermstrüwer*, Informationelle Selbstgefährdung, S. 366 ff., welcher für ein „rationalitätsförderndes Datenschutzrecht" plädiert, welches die Nutzer über die Konsequenzen ihres Umgangs mit den eigenen Daten aufklären, sowie Komplexität reduzieren und Rationalitätsdefizite z.B. in Form von Entscheidungsträgheit oder Überforderung bei langen Zeithorizonten kompensieren soll.

[1494] Instruktiv zum erlaubten Risiko im Risikovorsorgerecht: *Hoffmann-Riem*, AöR 1998, 513 (528 ff.) m.w.N.

Aus dieser Grundsatzentscheidung folgt dann auch, warum trotz vergleichbarer Defizite eine Übertragung der Beschränkungen des allgemeinen Verbraucherschutzrechts auf die datenschutzrechtliche Einwilligung abzulehnen ist: Anders als im Verbraucherschutzrecht ist es Teil der durch das Datenschutzrecht und die informationelle Selbstbestimmung geschützten Freiheit, eine objektiv schlechte oder unvernünftige Entscheidung über den Umgang mit den eigenen Daten zu treffen. Die Defizite der Einwilligung sind als Teil eines erlaubten und gesellschaftlich tolerierten Risikos zu werten, welches wir im Rahmen der allgemeinen Risikogesellschaft auf uns nehmen.[1495] Wie bei jedem solchen Risiko sollte versucht werden, es so weit wie möglich zu reduzieren, etwa durch die oben diskutierten Maßnahmen. Es sollte aber Abstand von der Illusion genommen werden, dass sich dieses Risiko gänzlich ausschließen oder beseitigen lassen wird.

2. Marktversagen im Datenschutz

Ein weiterer Ansatz, das Informations- und Machtgefälle zwischen Datenverarbeitern und Betroffenen zu reduzieren und einen effektiveren Datenschutz zu erhalten, liegt in allgemeinen Marktmechanismen. Sofern unter den Konsumenten eine Nachfrage nach gutem Datenschutz entsteht, wird dieser zu einem Bestandteil des Wettbewerbs und kann damit über den Erfolg der Verbreitung von Unternehmen mitbestimmen.[1496]

Freilich dürfen die Möglichkeiten dieser Selbstregulierung des Marktes nicht überschätzt werden. Angesichts der geringen Bedeutung, die dem Schutz ihrer Daten von den Betroffenen heute häufig beigemessen wird[1497], ist es nicht selbstverständlich, dass sich ein solches marktrelevantes Interesse am Datenschutz in absehbarer Zeit überhaupt ausbilden wird.[1498] Selbst wenn sich ein solches Interesse herausbildet, ist unklar, ob es sich insbesondere in Bezug auf soziale Netzwerke effektiv auswirken wird. Wie zuvor bereits gezeigt wurde, tendieren soziale Netzwerke zu einem natürlichen Monopol; gerade im Falle von Facebook ist diese Tendenz derart stark ausgeprägt, dass sogar ernsthaft über eine Verletzung des

---

[1495] Ausführlich zum Verhältnis von Informations- und Risikogesellschaft: *Hoffmann-Riem*, AöR 1998, 513 (528 f.) m.w.N.

[1496] Ausführlich: *Buchner*, Informationelle Selbstbestimmung, S. 131 ff.; vgl. auch *Härting/Schneider*, ZRP 2011, 233 (235).

[1497] Vgl. *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012, S. 104 ff.; *Bäcker*, Der Staat (51) 2012, 91 (112 f.); *Radlanski*, Das Konzept der Einwilligung, S. 222 f.; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 240 ff.

[1498] *Grimmelmann*, 94 Iowa L.Rev. 1137 (1178 ff.), 2008-2009; ausführlich hierzu aus spieltheoretischer und verhaltensökonomischer Perspektive *Hermstrüwer*, Informationelle Selbstgefährdung, S. 134 ff., 249 ff., 351.

Kopplungsverbots nachgedacht werden muss.[1499] Die Lock-In-Effekte durch die Vernetzung mit anderen und die in ein Profil investierte Arbeit erschweren den Wechsel und setzen eine große Wanderungsbewegung von Nutzern voraus, um einen effektiven Niedergang Facebooks zugunsten eines datenschutzfreundlicheren Konkurrenten wahrscheinlich zu machen. Ohne eine solche Wanderungsbewegung hat Facebook aber keinen ökonomischen Druck, um seine Datenschutzbestimmungen und –praktiken zu ändern.[1500]

Eine staatliche Regulierung zum Ausgleich dieses an Marktversagen grenzenden Zustands ist daher dringend erforderlich, um die Belange der informationellen Selbstbestimmung von Nutzern in sozialen Netzwerken zu schützen. Zugleich weist die Erkenntnis, dass es sich hierbei auch um Marktregulierung handelt, eindeutig darauf hin, dass es sich nicht nur um eine Aufgabe des Datenschutzrechts handeln kann. Vielmehr ist es auf eine Kooperation unter anderem mit dem Wettbewerbsrecht angewiesen, welches über Durchsetzungsinstrumente verfügt, um eine Einhaltung auch datenschutzrechtlicher Vorgaben sicherzustellen.[1501]

Die DS-GVO beschreitet in dieser Hinsicht bereits einen sehr guten Weg, indem sie die möglichen Bußgeldzahlungen für Datenschutzverstöße – in bestimmten Fällen – auf bis zu 20 Mio. Euro bzw. 4% des Jahresumsatzes eines Unternehmens erheblich erhöht hat.[1502] Daten und Informationen bedürfen eines besonderen Vorfeldschutzes, da nach ihrer Übermittlung oder Erhebung für den Betroffenen nur noch sehr wenige Kontrollmöglichkeiten hinsichtlich ihrer Verbreitung existieren.[1503] Speziell in sozialen Netzwerken kommt es zudem zu Gefährdungen der informationellen Selbstbestimmung Dritter, da zum Teil sogar sehr detaillierte Rückschlüsse auf Personen gezogen werden können, die sich nicht für eine Preisgabe ihrer Daten in dem Netzwerk entschieden haben. Auch über die selbstbestimmt Daten preisgebenden Nutzer können Anbieter sozialer Netzwerke wie Facebook umfassende

---

1499 Hierzu ausführlich oben unter D.III.2.b)cc).

1500 Sehr kritisch gegenüber einer Regulierung durch Marktmechanismen daher auch *Grimmelmann*, 94 Iowa L.Rev. 1137 (1178 ff.), 2008-2009; *Kutscha*, GR-Schutz im Internet, S. 44 f.; kritisch auch *Kühling/Martini*, EuZW 2016, 448 (450); *Hoffmann-Riem*, Innovation und Recht, S. 656; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 224 f.; 355 f.

1501 *Buchner*, Facebook zwischen BDSG und UWG, in: FS Köhler, S. 56 ff.; ausführlich zur Notwendigkeit wettbewerbsrechtlicher Maßnahmen, allerdings mit Fokus auf Google, *Newman*, 40 William Mitchell L. Rev., 849 (856 ff.), 2013-2014. *Hermstrüwer*, Informationelle Selbstgefährdung, S. 134 ff. bezeichnet persönliche Informationen durch geringe Erhebungs-, Reproduktions- und Distributionskosten insoweit als öffentliches Gut mit der Konsequenz eines faktischen Marktversagens, was staatliche Regulierung notwendig mache.

1502 *Dieterich*, ZD 2016, 260 (264 f.); *Faust/Spittka/Wybitul*, ZD 2016, 120 (120), allerdings mit sehr kritischen Anmerkungen zur möglichen Heranziehung des kartellrechtlichen Unternehmensbegriffs zur Bestimmung des maßgeblichen Jahresumsatzes; *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner, S. 438 f.

1503 Vgl. hierzu bereits grundlegend oben unter B.II.1.

Persönlichkeitsprofile erstellen, die in ihrer Detailliertheit weit über das hinausgehen, was der durchschnittliche Nutzer für möglich halten würde.[1504]

Nach dieser Problemanalyse erscheint es wenig vielversprechend, die Durchsetzung des Datenschutzrechts durch bloße Marktmechanismen und die freie Entscheidung der Nutzer zu erreichen. Der auf Freiheitsmaximierung zielende Ansatz, den Betroffenen „ins Zentrum der Datenverarbeitung" zu rücken und seine Selbst- und Mitbestimmungsrechte durch eine stärkere Fokussierung auf die Einwilligung zu stärken[1505], läuft Gefahr, zu einer bloßen Freiheitskulisse zu werden, in welcher die Betroffenen ihre Freiheit lediglich zur umfassenden Selbstentmündigung nutzen. Um dies zu verhindern, steht der Staat in der Verantwortung aus seiner Schutzpflicht, vergleichbar zum Verbraucherschutzrecht beschränkende Regelungen für die Datenverarbeitung durch datenverarbeitende Unternehmen zu erlassen und diese engmaschig zu kontrollieren und durchzusetzen.[1506]

Hierbei scheint ein bereichsspezifischer Ansatz unverzichtbar. Wie *Buchner* treffend herausarbeitet, bedeuten datenschutzrechtliche Generalklauseln, insbesondere Interessenabwägungsklauseln als Erlaubnistatbestände faktisch eine Verarbeitung von personenbezogenen Daten am Betroffenen vorbei.[1507] Der Komplexität der Datenverarbeitung in sozialen Netzwerken kann nicht dadurch begegnet werden, dass diese den privat handelnden Akteuren zur indivduellen Aushandlung überlassen wird. Vielmehr würden die Macht- und Informationsgefälle hier regelmäßig zu einer Lösung zu Lasten der informationellen Selbstbestimmung der Betroffenen führen, mit all den langfristigen Gefährdungen, die oben unter B.II.3 gezeigt wurden. Notwendig ist daher eine staatliche Regulierung, die jedenfalls im Ansatz nach den unter D.I.3 herausgearbeiteten Akteuren differenziert und klare Rahmenbedingungen für die Zulässigkeit einer Datenverarbeitung schafft. Diese Regelungen sind zu flankieren durch Maßnahmen des technischen Datenschutzes und einer Stärkung des Selbstdatenschutzes.[1508]

[1504] Hierzu bereits ausführlich oben unter B.II.; zu den Konsequenzen für die Informiertheit der Einwilligung s. oben unter D.III.2.b)aa).

[1505] So ausführlich *Buchner*, Informationelle Selbstbestimmung, S. 130 ff.

[1506] Vgl. auch *Kutscha*, GR-Schutz im Internet, S. 46 ff. m.w.N.; *Hermstrüwer*, Informationelle Selbstgefährdung, S. 387; *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner, S. 438 f. Zur staatlichen Infrastrukturverantwortung zur Gewährleistung einer selbstbestimmten Kommunikationsteilhabe auch bereits oben unter D.III.3.a).

[1507] *Buchner*, Informationelle Selbstbestimmung, S. 112, 118 ff.

[1508] Hierzu ausführlich oben unter D.III.3.

F. Zusammenfassende Thesen und Fazit

Die Arbeit beschäftigte sich mir der Frage, wie effektiv das bisherige nationale und zukünftige europäische Datenschutzrecht die informationelle Selbstbestimmung von Nutzern sozialer Netzwerke absichert. Ausgehend von den Datenverarbeitungsmöglichkeiten in sozialen Netzwerken wurden schwerpunktmäßig die Probleme der internationalen Anwendbarkeit des Datenschutzrechts, der Verantwortungsdiffusion in mehrseitigen Rechtsverhältnissen, des Rechts auf anonyme Nutzung sowie des Ausgleichs von Informations- und Machtgefällen in sozialen Netzwerken analysiert. Die Untersuchung erfolgte dabei erstmalig unter ausführlicher Berücksichtigung der endgültig verabschiedeten Fassung der DS-GVO und der sich aus dieser ergebenden Änderungen der Rechtslage in Bezug auf die betrachteten Fragestellungen.

I. Bestimmung des kollisionsrechtlich anwendbaren Datenschutzrechts

Bis zur Geltung der DS-GVO ab dem 25. Mai 2018 gemäß Art. 99 DS-GVO stellt sich die Frage nach dem auf soziale Netzwerke – insbesondere Facebook – anwendbaren nationalen Datenschutzrecht innerhalb der europäischen Union. Angesichts im Detail divergierender Schutzstandards ist die Frage von besonderer praktischer Bedeutung und derzeit Gegenstand verschiedener laufender Gerichtsverfahren, unter anderem eines durch das BVerwG angestrengten Vorlageverfahrens vor dem EuGH.[1509] Auch nach Geltung der DS-GVO und der durch sie bewirkten Rechtsvereinheitlichung bleiben die bisher im kollisionsrechtlichen Zusammenhang entwickelten Grundsätze zur Bestimmung der verantwortlichen Stelle im Rahmen der Art. 55 f. DS-GVO relevant, um die zuständige und federführende datenschutzrechtliche Aufsichtsbehörde zu bestimmen.[1510] Ob darüber hinaus Umsetzungsspielräume existieren, die eine nationale Konkretisierung der teilweise sehr allgemein gehaltenen Datenverarbeitungsvorschriften der DS-GVO im Rahmen der bisherigen §§ 11 ff. TMG gestatten, wird letztlich nur durch eine Vorlage an den EuGH zu klären sein.[1511]

Maßgeblich für die Anwendbarkeit deutschen Datenschutzrechts auf soziale Netzwerke ist bis zum 25. Mai 2018 § 1 Abs. 5 BDSG, welcher als zentralen rechtlichen Anknüpfungspunkt die verantwortliche Stelle für die Datenverarbeitung benennt. Wie in dieser Arbeit gezeigt wurde, ist hierbei nach der Rechtsprechung des EuGH zu den zugrundeliegenden Art. 2 und 4 DSRL von einem wirtschaftlich-funktionellen Verantwortlichkeitsbegriff auszugehen. Speziell für Facebook bedeutet dies eine zwingende Anwendbarkeit deutschen Datenschutzrechts innerhalb

[1509] BVerwG, ZD 2016, 393 (393 ff.).
[1510] Oben unter C.I.3.
[1511] Oben unter C.I.2.

Deutschlands. Der immer wieder versuchten Strategie Facebooks, sich auf die Anwendbarkeit irischen Datenschutzrechts zu berufen und sich damit zahlreichen datenschutzrechtlichen Pflichten zu entziehen, wurde damit die Grundlage entzogen.

In europarechtskonformer Auslegung war für die Bestimmung der verantwortlichen Stelle nach § 1 Abs. 5 BDSG stets entscheidend, wer die Kontrolle über die Zwecke und Mittel der Datenverarbeitung innehat. Im Verhältnis der *Facebook Inc.* in den USA und der *Facebook Ireland Ltd.* in Irland sprechen die deutlich überzeugenderen Argumente dafür, von einer entsprechenden Kontrolle durch die *Facebook Inc.* auszugehen. Dies hätte zur Folge, dass gemäß § 1 Abs. 5 S. 2 BDSG deutsches Datenschutzrecht zur Anwendung käme, da die verantwortliche Stelle für die Datenverarbeitung nicht in der Europäischen Union oder einem sonstigen Mitgliedstaat des EWR belegen wäre.[1512]

Mit der *Google*-Entscheidung vom Mai 2014 konkretisierte der EuGH indes den Begriff der verantwortlichen Stelle für die Herausforderungen einer globalen und arbeitsteiligen Datenökonomie. Hiernach ist auch eine solche Niederlassung als verantwortliche Stelle anzusehen, deren Tätigkeiten in einem wirtschaftlich untrennbaren Zusammenhang zu der Verarbeitung personenbezogener Daten durch die Hauptniederlassung stehen und die Rentabilität derselben maßgeblich mitbeeinflussen, selbst wenn die Tätigkeiten ansonsten nur untergeordneter Natur sind. Unter Zugrundelegung dieses fortentwickelten wirtschaftlich-funktionellen Verantwortlichkeitsbegriffs ist richtigerweise nunmehr auch die *Facebook Germany GmbH* als im Inland belegene verantwortliche Stelle im Sinne des § 1 Abs. 5 BDSG anzusehen. Dies begründet die Anwendbarkeit deutschen Datenschutzrechts aufgrund von § 1 Abs. 5 S. 1 letzter Hs. BDSG und zukünftig gegebenenfalls auch die Zuständigkeit deutscher Aufsichtsbehörden nach den Art. 55 f. DS-GVO i.V.m. § 18 f., 40 BDSG n.F. gemäß Art. 1 DSAnpUG-EU.[1513]

II. Datenschutzrechtliche Verantwortlichkeit in mehrseitigen Rechtsbeziehungen

Moderne digitale Datenverarbeitung erweist sich unter anderem in sozialen Netzwerken als komplexe arbeitsteilige und mehrseitige Rechtsbeziehung. Die klassische dichotome Aufteilung des Datenschutzrechts in Datenverarbeiter und Betroffenen stößt hierbei an ihre Grenzen, da oftmals keine alleinige und vollständige Kontrolle über Zwecke und Mittel der einzelnen Datenverarbeitungsschritte mehr besteht. Vielmehr wirken unterschiedliche Akteure

[1512] Oben unter C.II.4.a).
[1513] Oben unter C.I.3, C.II.4.b)bb) und C.II.4.b)cc).

unabhängig voneinander an denselben Datenverarbeitungen mit. Hieraus resultieren zahlreiche Unsicherheiten in der tatbestandlichen Bestimmung des Verantwortlichen, die auch durch die DS-GVO nicht zufriedenstellend gelöst werden, da diese die bisherige Legaldefinition des Verantwortlichen unverändert in Art. 4 Nr. 7 DS-GVO übernimmt.

In dieser Arbeit wurde gezeigt, dass die angemessene Antwort des Rechts auf diese Verantwortungsdiffusion auf Tatbestandsseite eine normative Verantwortungszurechnung auf Rechtsfolgenseite ist: Soweit unterschiedliche Akteure arbeitsteilig in einer Art und Weise zusammenarbeiten, dass keinem von ihnen eine vollständige Kontrolle über die Zwecke und Mittel der Datenverarbeitung zukommt, trifft sie dem Betroffenen gegenüber nach außen eine gesamtschuldnerische ordnungsrechtliche Verantwortlichkeit. Dieser auch von Art. 26 DS-GVO eingeschlagene Weg sichert die Steuerungsfähigkeit des Datenschutzrechts, indem klare Adressaten ordnungsrechtlicher Regelungen geschaffen und damit Betroffenenrechte effektiv geschützt werden. Sie erweist sich als angemessene Risikoverteilung, da es in der Sphäre der entsprechenden Datenverarbeiter liegt, eine andere Form der Datenverarbeitung zu wählen oder sich um eine klarere Aufteilung der Verantwortlichkeit zu bemühen.[1514]

Als zentrale datenverarbeitende Akteure in sozialen Netzwerken wurden die Anbieter, die Nutzer, private und öffentliche Fanpage-Betreiber, Verwender von Social PlugIns und Anbieter externer Inhalte wie Spiele und Apps betrachtet. Es konnte gezeigt werden, dass trotz der komplex organisierten Zusammenarbeit rechtlich klare Verantwortlichkeitszuschreibungen möglich sind und dass das geltende Datenschutzrecht mit den Herausforderungen sozialer Netzwerke umgehen kann. Hierbei wurden erstmalig die unterschiedlichen Akteure nicht nur vertieft für sich genommen betrachtet, sondern im Kontext zueinander in ein umfassendes und schlüssiges Verantwortlichkeitssystem in sozialen Netzwerken gestellt.

Speziell für die Anbieter sozialer Netzwerke besteht hiernach in aller Regel eine umfassende datenschutzrechtliche Verantwortlichkeit insbesondere auch für nutzergenerierte Inhaltsdaten, soweit diese – wie beispielsweise bei Facebook – zentraler Bestandteil des wirtschaftlichen Geschäftsmodells sind. Es ist unschädlich, dass die Anbieter keinen direkten Einfluss auf die Auswahl und den individuell intendierten Zweck der duch die Nutzer generierten Inhalte haben. Die Haftungsprivilegierungen der §§ 7 ff. TMG sowie die Grundsätze der Störerhaftung sind nicht auf die datenschutzrechtliche Verantwortlichkeit zu übertragen.[1515]

[1514] Oben unter D.I.2.b).
[1515] Oben unter D.I.3.a).

Nutzer sozialer Netzwerke fallen nicht unter das sogenannte Haushaltsprivileg gemäß § 1 Abs. 2 Nr. 3 BDSG bzw. Art. 2 Abs. 2 lit. c) DS-GVO, wenn sie personenbezogene Daten Dritter in ein soziales Netzwerk übermitteln. Das Haushaltsprivileg bewirkt zwar eine wichtige Sicherung der freien Kommunikation und privaten Selbstververwirklichung, indem es die Verwendung personenbezogener Daten Dritter in einem rein privaten und familiären Kontext von dem Regelungsbereich des Datenschutzrechts ausnimmt. Die Übermittlung solcher Daten in soziale Netzwerke stellt aber eine strukturelle Gefährdung der informationellen Selbstbestimmung der betroffenen Dritten dar, da die Daten weit über den familiären und persönlichen Umkreis des sie verwendenden Nutzers hinaus verbreitet werden können. In einer grundrechtskonformen Auslegung, die die praktischen Gegebenheiten sozialer Netzwerke und des Internets angemessen berücksichtigt, ist das Haushaltsprivileg daher entsprechend teleologisch zu reduzieren. Die aus der datenschutzrechtlichen Verantwortlichkeit der Nutzer resultierenden Pflichten sind freilich auf solche Pflichten beschränkt, die die Nutzer rechtlich erfüllen können, da das Recht keine unmöglichen Pflichten auferlegen darf.[1516]

Die Betreiber von Fanpages haben keine Kontrolle über die Zwecke und Mittel, für welche die beim Besuch ihrer Seiten entstehenden Bestands- und Nutzungsdaten von Nutzern verwendet werden. Sie sind nach hier vertretener Ansicht dennoch nach den Grundsätzen des Zweckveranlassers ordnungsrechtlich verantwortlich, soweit sie hinreichende Kenntnis von rechtswidrigen Verarbeitungen dieser Daten haben können und von diesen profitieren. Wie gezeigt wurde, ist dies im Fall von Facebook-Fanpages zu bejahen. Die Betreiber von Fanpages können somit Adressaten ordnungsrechtlicher Verfügungen der Datenschutzbehörden sein, die ihnen auferlegen, die Rechtmäßigkeit der Datenverarbeitung sicherzustellen oder andernfalls den Betrieb der Fanpage zu unterlassen.[1517]

Die Verwender von Social PlugIns können durch die Art der technischen Integration des PlugIns in die eigene Webseite selbst entscheiden, ob es zu einer automatischen Datenübermittlung von Bestands- und Nutzungsdaten an die Anbieter sozialer Netzwerke kommt. Sie sind damit mittelbar verantwortlich für eine mögliche rechtswidrige Datenverarbeitung durch den Social PlugIn Anbieter. Zur rechtlichen Absicherung ist ihnen zu empfehlen, auf technische Lösungen wie die „Zwei-Klick-Lösung“ auszuweichen, welche eine Einwilligung der das PlugIn verwendenden Nutzer sicherstellen.[1518]

[1516] Oben unter D.I.3.b).
[1517] Oben unter D.I.3.c).
[1518] Oben unter D.I.3.d).

Die Grundsätze der datenschutzrechtlichen Verantwortlichkeit sind auch unverändert auf die Anbieter externer Inhalte – wie beispielsweise Spiele oder sonstige Apps – in sozialen Netzwerken anwendbar. Soweit sie selbst personenbezogene Nutzerdaten verarbeiten, sind sie hierfür unproblematisch verantwortlich. Auch die hier zu Fanpage-Betreibern und Social PlugIn Verwendern entwickelten Grundsätze sind auf sie zu übertragen, soweit es zu vergleichbaren Datenübermittlungen kommt. An der Rechtmäßigkeit der Datenverarbeitung von Anbietern externer Inhalte bestehen zumindest im Fall von Facebook zum Teil erhebliche Zweifel, denen in einer Einzelfallprüfung nachzugehen ist.[1519]

III. Persönlichkeitsrechtsschutz und effektive Rechtsverfolgung

Soziale Netzwerke können in der heutigen Zeit eine besondere Bedeutung für die individuelle Persönlichkeitsbildung haben, dadurch dass Selbst- und Fremdbilder entwickelt und präsentiert werden.[1520] Dabei kommt es zu einem Konflikt zwischen der Ermöglichung einer anonymen oder jedenfalls pseudonymen Nutzung – welche durch § 13 Abs. 6 TMG garantiert wird – und dem Interesse an einer effektiven Rechtsverfolgung im Falle von Rechtsverletzungen.

Der Umfang und die grundsätzliche Anwendbarkeit des § 13 Abs. 6 TMG in Bezug auf Nutzerprofile bei Facebook war zuletzt Gegenstand verwaltungsgerichtlicher Entscheidungen des *VG* und *OVG Hamburg* im einstweiligen Rechtsschutz[1521] und hängt in der endgültigen gerichtlichen Klärung von dem beim EuGH anhängigen Vorlageverfahren des BVerwG ab.[1522] Wie in dieser Arbeit gezeigt wurde, ist § 13 Abs. 6 TMG kollisionsrechtlich innerhalb des deutschen Rechtsraums auf Facebook anwendbar und garantiert gegenüber anderen Nutzern ein unbedingtes Recht auf pseudonyme Nutzung. Gegenüber dem Anbieter des sozialen Netzwerks ist dagegen eine teleologische Reduktion vorzunehmen, da diesem nicht zugemutet werden kann, mit einer anonymen Person Verträge zu schließen. Dies gilt umso mehr im Lichte der zuvor in dieser Arbeit begründeten umfassenden datenschutzrechtlichen Verantwortlichkeit der Anbieter kommerzieller sozialer Netzwerke für nutzergenerierte Inhaltsdaten.[1523]

Die DS-GVO enthält zwar kein ausdrückliches Recht auf pseudonyme Nutzung von Telemedien und dem Internet im Allgemeinen. Nach hier vertretener Auffassung lässt sich ein solches Recht indes aus den Vorschriften der Art. 5 Abs. 1 lit. b) und c), 25 und 32 DS-GVO

[1519] Oben unter D.I.3.e).
[1520] Oben unter B.I. und B.II.3.a).
[1521] VG Hamburg, ZD 2016, 243 (243 ff.); ZD 2016, 450 (451 ff.).
[1522] BVerwG, ZD 2016, 393 (393 ff.).
[1523] Oben unter D.II.

sowie Art. 7 und 8 GrCH ableiten. Die hier entwickelten Thesen zur Ermöglichung einer pseudonymen Nutzungsmöglichkeit gegenüber anderen Nutzern bewahren daher auch nach Geltung der DS-GVO ihre Bedeutung.[1524]

IV. Ausgleich struktureller Informations- und Machtgefälle

In sozialen Netzwerken treten die im digitalen Kontext weit verbreiteten Schwierigkeiten einer selbstbestimmten Einwilligung im Angesicht von erheblichen Informations- und Machtgefällen besonders deutlich zu Tage: Die Komplexität der Datenverarbeitungsbedingungen und -konsequenzen, ein verbreitetes datenschutzrechtliches Desinteresse und der soziale Druck zur Teilnahme lassen es mehr als fragwürdig erscheinen, ob eine hinreichend bestimmte, freiwillige und informierte Einwilligung tatsächlich möglich und nicht nur eine bloße Fiktion ist.[1525] Gleichzeitig erweist sich aber der vollständige defätistische Verzicht auf die Möglichkeit zu einer Einwilligung angesichts der Vielschichtigkeit des Grundrechts auf informationelle Selbstbestimmung als keine gangbare Lösung, würde dies doch eine unverhältnismäßige Beschränkung der Freiheit bedeuten, eigene Informationen preiszugeben.[1526]

Die Einwilligung in sozialen Netzwerken befindet sich somit in dem Dilemma, dass sie einerseits nicht realisierbar erscheint, andererseits aber unverzichtbar ist. Auch die DS-GVO bietet keine entscheidenden neuen Impulse zur Lösung dieser Problematik, sondern beseitigt vor allem kleinere Abgrenzungsprobleme, die bisher insbesondere zwischen der Einwilligung nach dem BDSG und dem TMG bestanden.[1527]

Erfolgsversprechende unterstützende Maßnahmen zur Sicherung der informationellen Selbstbestimmung liegen in der Stärkung des Selbstdatenschutzes etwa durch die Verbesserung des Datenschutzes durch Technik bzw. *privacy by design*, einer zeitlichen Beschränkung der Einwilligung, der Einführung eines Rechts auf Datenportabilität sowie in der Stärkung von Verbandsklagerechten. Diese bereits im bisherigen nationalen Recht angelegten Strategien werden durch die DS-GVO begrüßenswerterweise fortgeführt und teilweise vertieft. Dennoch bleibt die Effektivität dieser Maßnahmen letztlich zweifelhaft: Datenschutz durch Technik lindert überwiegend nur die Symptome einer schlecht informierten, unfreiwilligen „Einwilligung“, schafft aber nicht notwendig mehr Selbstbestimmung. Insbesondere bei dem in Art. 20 DS-GVO normierten Recht auf Datenportabilität wird zudem abgewartet werden

[1524] Oben unter D.II.2.a).
[1525] Oben unter D.III.2.b).
[1526] Oben unter D.III.4.a).
[1527] Oben unter D.III.2.a).

müssen, wie es konkret in der Praxis angewendet werden wird und ob es in sozialen Netzwerken bestehende Lock-In Effekte sowie bei Nutzern bestehende Status Quo Biase aufbrechen können wird.[1528]

Im Ergebnis präsentiert sich die Gefahr, eine schlechtinformierte, fremdbestimmte Entscheidung im Rahmen der Einwilligung zur Nutzung sozialer Netzwerke zu treffen, als ein in einer freien Gesellschaft nicht vollkommen ausschließbares Risiko. Nutzer müssen durch die hier aufgezeigten Maßnahmen bei ihrer Entscheidungsfindung unterstützt und Anbieter sozialer Netzwerke für Missbrauch zur Verantwortung gezogen werden. Die Komplexität der Entscheidung durch weitergehende paternalistische Maßnahmen zu reduzieren, ist dagegen in den meisten Fällen weder verhältnismäßig noch zielführend: Es ist nicht die Aufgabe des Staates, die Bürger ausschließlich zum Schutz vor sich selbst zu einem aus staatlicher Sicht „vernünftigen“ Verhalten zu zwingen. Paternalistische Regelungen und ordnungsrechtliche Verbote sind daher streng danach zu differenzieren, ob ein selbstbestimmtes Verhalten einer Person nur dieser Person selbst schadet oder auch Dritte gefährdet. Dabei darf die Selbstbestimmung nicht allein deshalb in Frage gestellt werden, weil es sich von außen betrachtet um eine unvernünftige oder schlecht informierte Entscheidung handelt; ein gerechtfertiger Ansatzpunkt für paternalistische Regulierung besteht lediglich dort, wo die Selbstbestimmtheit einer Handlung objektiv eingeschränkt ist, etwa aufgrund von Krankheit, Täuschung oder Minderjährigkeit.[1529]

V. Das Datenschutzrecht als Risikovorsorgerecht

Moderne digitale Datenverarbeitung birgt sowohl erhebliche Chancen und Potentiale als auch Risiken. Soziale Netzwerke stellen hierbei keine Ausnahme dar.[1530] Unterschiedliche Kombinationsmöglichkeiten und neuartige Analysemethoden erlauben, aus beliebigen Daten immer neue Informationen zu kreieren.[1531] Einmal übermittelte Daten sind häufig der Kontrolle des Betroffenen dauerhaft entzogen. Ein effektiver Persönlichkeitsrechtsschutz muss daher bereits auf der Ebene der Daten und im Vorfeld von konkreten Persönlichkeitsgefährdungen ansetzen. Es kann jedoch nicht die Aufgabe des Datenschutzrechts sein, alle potentiellen Risiken insbesondere für die informationelle Selbstbestimmung Betroffener auszuschließen. Datenschutzrecht ist daher kein Risikoausschließungs-, wohl aber ein Risikovorsorgerecht.

[1528] Oben unter D.III.3.a).
[1529] Oben unter D.III.4.
[1530] Oben unter B.II.3.
[1531] Oben unter B.II.1.

Die Grenzen der Leistungsfähigkeit des Datenschutzrechts dürfen nicht verkannt werden: durch die heutige Ubiquität der Datenverarbeitung werden fast alle Lebensbereiche von Datenverarbeitungen berührt. Es wäre vermessen und unpraktikabel, wollte das Datenschutzrecht versuchen, alle hiermit verbundenen Probleme selbst zu lösen. Datenschutzrecht ist vielmehr in zunehmendem Maße eine Querschnittsmaterie, die für eine effektive Regulierung auf eine enge Verzahnung mit anderen Rechtsgebieten wie dem Wettbewerbsrecht und dem Kartellrecht angewiesen ist. Die DS-GVO geht insoweit wichtige erste Schritte; dennoch ist eine noch engere Kooperation in Zukunft unabdingbar.[1532]

Die Geschwindigkeit des technischen Fortschritts und das Bestreben, allen zukünftigen Risiken begegnen zu können, dürfen nicht dazu verleiten, das Datenschutzrecht übermäßig abstrakt zu gestalten und sich konkreter Regelungen zu enthalten. Zwar ist es im Ausgangspunkt richtig, dass das Datenschutzrecht technologieneutral sein muss, da der Schutzumfang nicht von der konkret verwendeten Technologie abhängen kann. Dennoch bedarf es hinreichend klarer Entscheidungen von Interessenskonflikten, um die Verantwortlichkeit des demokratisch legitimierten Gesetzgebers nicht weitgehend an die Exekutive, Judikative und private Akteure zu delegieren. Die DS-GVO erweist sich insoweit an vielen Stellen als zu vage und konkretisierungsbedürftig. Wenngleich einheitliche rechtliche Regelungen im Sinne der Rechtsklarheit zu begrüßen sind, wird dieser Zweck dort verfehlt, wo durch unbestimmte, hochabstrakte Regelungen Rechtsunsicherheit geschaffen wird. Ein Datenschutzrecht, das als Querschnittsmaterie zahlreiche andere Lebensbereiche berührt, bedarf auch bereichsspezifischer Regelungen, um der Komplexität unterschiedlicher Lebenssachverhalte gerecht zu werden. Dies ist durch die DS-GVO bisher nicht hinreichend gewährleistet.[1533] Für die Zukunft bleibt daher nur zu hoffen, dass die DS-GVO auf europäischer Ebene weiter konkretisiert werden wird. In der Zwischenzeit erscheint es jedenfalls aus der Perspektive dogmatischer Klarheit wünschenswert, auf bisherige Fallgruppen zurückzugreifen, die anhand des bereichsspezifischen, konkreteren nationalen Datenschutzrechts in Umsetzung der europäischen DSRL entwickelt wurden.[1534]

VI. Fazit

Die sich rasant entwickelnde ubiquitäre Datenverarbeitung im Allgemeinen und die Datenverarbeitung im Zusammenhang mit sozialen Netzwerken im Speziellen stellen das

[1532] Oben unter E.II.2.
[1533] Oben unter E.I.1.
[1534] Oben unter C.I.2 und D.I.3.

europäisierte Datenschutzrecht vor erhebliche Herausforderungen. Globale Akteure und dezentralisierte Prozesse führen zu einer Verantwortungsdiffusion, die nicht nur kollisionsrechtliche Probleme schafft, sondern auf tatbestandlicher Ebene eindeutige Verantwortungszuweisung in vielen Fällen unmöglich macht. Zeitaufwändige parlamentarische Prozesse zur Anpassung des Rechts scheinen dem sich schnell und dezentral entwickelnden technologischen Fortschritt nur gelähmt hinterher zu laufen.

Diese Arbeit hat gezeigt, dass diese Probleme zwar ernst zu nehmen sind, es aber verfehlt wäre, dem Datenschutzrecht deswegen seine Steuerungsfähigkeit abzusprechen und es für gescheitert oder jedenfalls hoffnungslos veraltet zu erklären. Vielmehr erweisen sich sowohl das bisherige nationale als auch das zukünftige europäische Datenschutzrecht als hinreichend flexibel und fähig, um auch jene Probleme sozialer Netzwerke zu lösen, die bei Erlass des bisherigen Datenschutzrechts nicht einmal im Ansatz absehbar waren. Dennoch sind weitere Forschung und Schritte des Gesetzgebers erforderlich, um das ungelöste Dilemma der Einwilligung im digitalen Kontext praktisch zu entschärfen.

Durch die DS-GVO wurde ein großer Schritt in die richtige Richtung getätigt, indem die europäische Datenschutzgesetzgebung vereinheitlicht und für die Herausforderungen durch moderne digitale Datenverarbeitung sensibilisiert wurde. Die Aufgabe für die Zukunft ist es nunmehr, die teilweise sehr abstrakten und vagen Regelungen der DS-GVO bereichsspezifisch zu konkretisieren und somit Rechtssicherheit zu schaffen. Diese Arbeit hat hierfür in den jeweils diskutierten Problemen wichtige Ansätze geliefert, auf denen aufgebaut werden kann.

Anhänge: Literatur- & Materialverzeichnis

Anhang 1: Literaturverzeichnis

Albers, Marion	Information als neue Dimension im Recht, Rechtstheorie (33) 2002, S. 61-89
Dies.	Informationelle Selbstbestimmung, 1. Auflage, Baden-Baden 2005
Dies.	Grundrechtsschutz der Privatheit, DVBl. 2010, S. 1061-1069
Dies.	Umgang mit personenbezogenen Informationen und Daten, in: *Hoffmann-Riehm/Schmidt-Aßmann/Voßkuhle* (Hrsg.), Grundlagen des Verwaltungsrechts, Band 2, § 22, 2. Auflage, München 2012
Arning, Marian / Moos, Flemming	Location Based Advertising – Datenschutzkonforme Verwendung von Ortsdaten bei verhaltensbezogener Online-Werbung, ZD 2014, S. 126-133
Ders. / Ders.	Big Data bei verhaltensbezogener Online-Werbung – Programmatic Buying und Real Time Advertising, ZD 2014, S. 242-248
Auernhammer, Herbert (Begr.)	Kommentar zum Bundesdatenschutzgesetz – Nebengesetze, *Eße/Kramer/Lewinsky* (Hrsg.), 4. Auflage, Köln 2014 (zitiert als: *Bearbeiter*, in: Auernhammer)
Bamberger, Heinz Georg / Roth, Herbert (Hrsg.)	Kommentar zum Bürgerlichen Gesetzbuch, Band 2, 3. Auflage, München 2012 (zitiert als: *Bearbeiter*, in: Bamberger/Roth, BGB, Bd. 2)
Ders. / Ders. (Hrsg.)	Kommentar zum Bürgerlichen Gesetzbuch, Band 3, 3. Auflage, München 2012 (zitiert als: *Bearbeiter*, in: Bamberger/Roth, BGB, Bd. 3)
Bäcker, Matthias	Die Vertraulichkeit der Internetkommunikation, in: *Rensen/Brink* (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts – erörtert von den wissenschaftlichen Mitarbeitern, 1. Auflage, Berlin 2009, S. 99-136
Ders.	Grundrechtlicher Informationsschutz gegen Private, Der Staat (51) 2012, S. 91-116
Beckendorf, Ingo	Belgien: Facebook darf keine Daten von Nicht-Mitgliedern sammeln, MMR-Aktuell 2015, 374256, Ausgabe 24/2015 vom 15. Dezember 2015
Bender, Gunnar	Informationelle Selbstbestimmung in sozialen Netzwerken, K&R 2013, S. 218-220

Beyvers, Eva / Herbrich, Tilman — Das Niederlassungsprinzip im Datenschutzrecht – am Beispiel von Facebook; Der neue Ansatz des EuGH und die Folgen, ZD 2014, S. 558-562

Bieber, Christoph — Soziale Netzwerke als neue Arena politischer Kommunikation, in: *Bieber/Eifert/Groß/Lamla* (Hrsg.), Soziale Netzwerke in der digitalen Welt – Das Internet zwischen egalitärer Teilhabe und ökonomischer Macht, 1. Auflage Frankfurt a.M. 2009, S. 53-64.

Boehme-Neßler, Volker — Big Data und Demokratie – Warum Demokratie ohne Datenschutz nicht funktioniert, DVBl. 2015, S. 1282-1287

Ders. — Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht, NVwZ 2014, S. 825-830

Boos, Carina — Datenweitergabe an und durch Spieleanbieter auf Facebook – zugleich Anmerkung zu LG Berlin, Urt. v. 28.10.2015, Az. 16 O 60/13, VuR 2015, S. 92-98

Britz, Gabriele — Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: *Hoffmann-Riehm* (Hrsg.), Offene Rechtswissenschaft, 1. Auflage, Tübingen 2010, S. 562-596 (zitiert: *Britz*, Informationelle Selbstbestimmung)

Bräutigam, Peter — Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten, MMR 2012, S. 635 - 641

Borges, Georg — Der neue Personalausweis und der elektronische Identitätsnachweis, NJW 2010, S. 3334-3339

Bosesky, Pino / Brüning, Christoph — Verständnis und Schutz von digitaler Privatheit im nationalen Recht, in: *Hill/Schliesky* (Hrsg.), Die Neubestimmung der Privatheit – E-Volution des Rechts- und Verwaltungssystems IV, 1. Auflage, Baden-Baden 2014, S. 79-108

Brühann, Ulf — Mindeststandards oder Vollharmonisierung des Datenschutzes in der EG, EuZW 2009, S. 639-644

Buchholtz, Gabriele — Das „Recht auf Vergessen" im Internet – eine Herausforderung für den demokratischen Rechtsstaat, AöR 2015, S. 121-153

Buchner, Benedikt — Informationelle Selbstbestimmung im Privatrecht, 1. Auflage, Tübingen 2006

Ders. — Facebook zwischen BDSG und UWG, in: *Alexander u.a.* (Hrsg.), Festschrift für Helmut Köhler zum 70. Geburtstag, München 2014

Bull, Hans Peter — Persönlichkeitsschutz im Internet: Reformeifer mit neuen Ansätzen, NVwZ 2011, S. 257-263

Ders. — Netzpolitik: Freiheit und Rechtsschutz im Internet, 1. Auflage, Baden-Baden 2013

von Burgsdorff, Christoph — Die Umsetzung der EG-Datenschutzrichtlinie im nicht-öffentlichen Bereich, 1. Auflage, Frankfurt a.M. 2003

Caspar, Johannes — Nutzung des Web 2.0 – zwischen Bürgernähe und Geschwätzigkeit? Einsatz von Web 2.0-Plattformen durch öffentliche Stellen am Beispiel der Polizei, ZD 2015, S. 12-17

Ders. — Klarnamenpflicht versus Recht auf pseudonyme Nutzung, ZRP 2015, S. 233-237

Cebulla, Manuel — Umgang mit Kollateraldaten – Datenschutzrechtliche Grauzone für verantwortliche Stellen, ZD 2015, S. 507-512

Chmelik, Thomas — Social Network Sites - Soziale Netzwerke: Verantwortlichkeit für nutzergenerierte Inhalte unter besonderer Berücksichtigung der Störerhaftung, 1. Auflage, Baden-Baden 2016

(zitiert als: *Chmelik*, Social Network Sites)

Dammann, Ulrich — Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovation, ZD 2016, S. 307-314

Däubler, Wolfgang / Klebe, Thomas / Wedde, Peter / Weichert, Thilo (Hrsg.) — Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG, 4. Auflage, Frankfurt a.M. 2014

(zitiert als: *Bearbeiter*, in: DKWW)

Del Vicario, Michaela / Bessi, Allessandro u.a. — The spreading of misinformation online, PNAS 2016, 113 (3), S. 554-559; vgl. auch http://www.pnas.org/content/113/3/554.full.pdf

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) — DIVSI U25-Studie – Kinder, Jugendliche und Erwachsene in der digitalen Welt, Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVIS), Hamburg, Februar 2014

(zitiert als: *DIVSI*, U25-Studie v. Februar 2014)

Dieterich, Thomas — Canvas Fingerprinting – Rechtliche Anforderungen an neue Methoden der Nutzungsprofilerstellung, ZD 2015, S. 199-244.

Ders.	Rechtsdurchsetzungsmöglichkeiten der DS-GVO – Einheitlicher Rechtsrahmen führt nicht zwangsläufig zu einheitlicher Rechtsanwendung, ZD 2016, S. 260-266
Eichenhofer, Johannes	Privatheit im Internet als Vertrauensschutz – Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz, Der Staat (55) 2016, S. 41-67
Eidenmüller, Horst	Liberaler Paternalismus, JZ 2011, S. 814-821
Eifert, Martin	Zweckvereinbarkeit statt Zweckbindung, in: *Gropp/Lipp/Steiger* (Hrsg.), Rechtswissenschaft im Wandel – Festschrift des Fachbereichs Rechtswissenschaft zum 400jährigen Gründungsjubiläum der Justus-Liebig-Universität Gießen, 1. Auflage, Tübingen 2007, S. 139-152
Ders.	Regulierungsstrategien, in: *Hoffmann-Riehm/Schmidt-Aßmann/Voßkuhle* (Hrsg.), Grundlagen des Verwaltungsrechts, Band 1, § 19, 2. Auflage, München 2012
Engel-Flechsig, Stefan / Maennel, Frithjof A. / Tettenborn, Alexander (Hrsg.)	Beck'scher IuKDG-Kommentar – Informations- und Kommunikationsdienstegesetz, 1. Auflage, München 2001 (zitiert als: *Autor*, in: Beck'scher IuKDG-Kommentar)
Englerth, Markus / Hermstrüwer, Yoan	Die Datenkrake als Nutztier der Strafverfolgung, RW 2013, S. 326-359
Erd, Rainer	Datenschutzrechtliche Probleme sozialer Netzwerke, NVwZ 2011, S. 19-22
Ernst, Stefan	Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, S. 1917-1919
Faust, Sebastian / Spittka, Jan / Wybitul, Tim	Millardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, ZD 2016, S. 120-125
Fehling, Michael	Informelles Verwaltungshandeln, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, 2. Auflage, München 2012
Ders.	Evolving Law and Economics of Internet Privacy in the Evolving Technological Environment, in: Eger/Oeter/Voigt (Hrsg.), Economic Analysis of International Law, Contributions to the XIIIth Travemünde Symposium on

	the Economic Analysis of Law (March 29-31, 2012), 1. Auflage, Tübingen 2014, S. 99-115
Ders.	Informational Privacy im Spiegel unterschiedlicher Rechtskulturen, in: Fehling/Schliesky, zusammen mit dem Deutschen Institut für Vertrauen und Sicherheit im Internet (Hrsg.), S. 121-148, Baden-Baden – *Erscheinen in Vorbereitung*
Feldmann, Thorsten	K&R-Kommentar, Anmerkung zum Urteil des BGH vom 25.10.2011, Az. VI, ZR 93/10 – Blotspot-Entscheidung, K&R 2012, S. 113-116.
Geminn, Christian / Roßnagel, Alexander	„Privatheit" und „Privatsphäre" aus der Perspektive des Rechts – ein Überblick, JZ 2015, S. 703-708
Gercke, Marco	Die Entwicklung des Internetstrafrechts 2011/2012, ZUM 2012, S. 625-636
Gerhold, Sönke	Möglichkeiten und Grenzen der sogenannten „Facebookfahndung", ZIS 2015, S. 156-174
Gierschmann, Sibylle	Was „bringt" deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber Rechtsunsicherheit bleibt, ZD 2016, S. 51-55
Gola, Peter / Schulz, Sebastian	DS-GVO – Neue Vorgaben für den Datenschutz bei Kindern? Überlegungen zur einwilligungsbasierten Verarbeitung von personenbezogenen Daten Minderjähriger, ZD 2013, S. 475-481
Gola, Peter / Klug, Christoph / Körffer, Barbara	BDSG – Bundesdatenschutzgesetz, Kommentar, 12. Auflage, München 2015 (zitiert als: *Gola/Schomerus*, BDSG)
Gola, Peter / Lepperhoff, Niels	Reichweite des Haushalts- und Familienprivilegs bei der Datenverarbeitung; Aufnahme und Umfang der Ausnahmereglung in der DS-GVO, ZD 2016, S. 9-12
Greve, Felix	Die staatliche Gewährleistungsverantwortung für offene Standards – Interoperabilität von Dateiformaten als Voraussetzung des e-Governments, Problem des Wettbewerbsrechts und telekommunikationsrechtliche Notwendigkeit, 1. Auflage, Baden-Baden 2015
Greve, Holger / Schärdel, Florian	Der digitale Pranger – Bewertungsportale im Internet, MMR 2008, S. 644-650

Greve, Holger — Drittwirkung des grundrechtlichen Datenschutzes im digitalen Zeitalter, in: *Franzius u.a.* (Hrsg.), Beharren. Bewegen. – Festschrift für Michael Klopfer zum 70. Geburtstag, Berlin 2013, S. 665-677

Grimmelmann, James — Saving Facebook, Iowa L. Rev. 94, 2008-2009, S.1137-1206

Guggenberger, Nikolas — Das Netzwerkdurchsetzungsgesetz in der Anwendung, NJW 2017, S. 2577-2582

Gurlit, Elke — Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, S. 1035-1041

Gusy, Christoph — Informationelle Selbstbestimmung und Datenschutz: Fortführung oder Neuanfang?, KritV 2000, S. 52-64

Ders. — Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Neuer Grundrechtsname oder neues Grundrechtsschutzgut?, DuD 2009, S. 33-41

Ders. — Polizei- und Ordnungsrecht, 9. Auflage, Tübingen 2014

Haase, Martin Sebastian — Datenschutzrechtliche Fragen des Personenbezugs – Eine Untersuchung des Anwendungsbereichs des deutschen Datenschutzrechts und seiner europarechtlichen Bezüge, 1. Auflage, Tübingen 2015

(zitiert als: *Haase*, Datenschutzrechtliche Fragen des Personenbezugs)

Haratsch, Andreas / Koenig, Christian / Pechstein, Matthias — Europarecht, 9. Auflage, Tübingen 2014

Härting, Niko — Datenschutz zwischen Transparenz und Einwilligung – Datenschutzbestimmungen bei *Facebook*, *Apple* und *Google*, CR 2011, S. 169-175

Ders. — Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, S. 2065-2072

Ders. / Schneider, Jochen — Das Dilemma der Netzpolitik, ZRP 2011, S. 233-236

Heckmann, Dirk — Persönlichkeitsschutz im Internet – Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderung für Ehrschutz und Profilschutz, NJW 2012, S. 2631-2635

Hermstrüwer, Yoan	Informationelle Selbstgefährdung – Zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung, 1. Auflage, Tübingen 2016 (zitiert als: *Hermstrüwer*, Informationelle Selbstgefährdung)
Hill, Hermann	Aus Daten Sinn machen: Analyse- und Deutungskompetenzen in der Datenflut, DÖV 2014, S. 213-222
Hoeren, Thomas	Das Telemediengesetz, NJW 2007, S. 801-806
Ders.	Unterlassungsansprüche gegen Host-Provider – die Rechtslage nach dem Ricardo-/Rolex-Urteil des BGH, in: *Wackerbarth u.a.* (Hrsg.), Festschrift für Ulrich Eisenhardt zum 70. Geburtstag, 1. Auflage, Müchen 2007, S. 243-254 (zitiert als: *Hoeren*, in: FS Eisenhardt)
Ders. / Sieber, Ulrich/ Holznagel, Bernd	Handbuch Multimedia-Recht, 42. Ergänzungslieferung, München 2015. (zitiert als: *Bearbeiter*, in: Hoeren/Sieber/Holznagel, Hdb. Multimediarecht)
Ders. / Bensinger , Viola (Hrsg.)	Haftung im Internet – Die neue Rechtslage, 1. Auflage, Baden-Baden 2014 (zitiert: *Bearbeiter*, in: Hoeren/Bensinger)
Hoffmann, Christan / Schulz, Sönke / Brackmann, Franziska	Die öffentliche Verwaltung in den sozialen Medien? Zulässigkeit behördlicher Facebook-Fanseiten, ZD 2013, S. 122-126
Hoffmann-Riem, Wolfgang	Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR (123) 1998, S. 513-540
Ders.	Regelungsstrukturen für öffentliche Kommunikation im Internet, AöR 2012, S. 508-544
Ders.	Rechtsformen, Handlungsformen, Bewirkungsformen, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, § 33, 2. Auflage, München 2012
Ders.	Innovation und Recht – Recht und Innovation, Recht im Ensemble seiner Kontexte, 1. Auflage, Tübingen 2016
Hollenders, Anna-Sophie	Mittelbare Verantwortlichkeit von Intermediären im Netz, 1. Auflage, Baden-Baden 2012 (zitiert: *Hollenders*, Mittelbare Verantwortlichkeit)
Hornung, Gerrit /	Ein Recht auf Vergessenwerden?, JZ 2013, S. 163-170

Hofmann/Kai

Hornung, Gerrit — Europa und darüber hinaus – Konzepte für eine Neuregelung des Datenschutzes im Internet und in sozialen Netzwerken, in: *Hill/Schliesky* (Hrsg.), Neubestimmung der Privatheit, 1. Auflage, Baden-Baden 2014, S. 123-151

Ders. / Goeble, Thilo — „Data Ownership“ im vernetzten Automobil - Die rechtliche Analyse des wirtschaftlichen Werts von Automobildaten und ihr Beitrag zum besseren Verständnis der Informationsordnung, CR 2015, S. 265-273

Jandt, Silke / Roßnagel, Alexander — Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz?, MMR 2011, S. 637-642

Dies. / Ders. — Datenschutz in Social Networks: Kollektive Verantwortlichkeit für die Datenverarbeitung, ZD 2011, S. 160-166

Joecks, Wolfgang / Miebach, Klaus (Hrsg.) — Münchener Kommentar zum StGB, Band 7 Nebenstrafrecht II, 2. Auflage, München 2015

(zitiert als: *Bearbeiter*, in: MüKo StGB, Bd. 7)

Kalscheuer, Fiete / Hornung, Christian — Das Netzwerkdurchsetzungsgesetz – Ein verfassungswidriger Schnellschuss, NVwZ 2017, S. 1721-1725

Kamp, Johannes — Personenbewertungsportale – Eine datenschutzrechtliche und äußerungsrechtliche Untersuchung unter besonderer Berücksichtigung des Lehrerbewertungsportals spickmich.de, 1. Auflage, München 2011

(zitiert als: *Kamp*, Personenbewertungsportale)

Karg, Moritz / Thomsen, Sven — Tracking und Analyse durch Facebook – Das Ende der Unschuld, DuD 2012, S. 729-736

Ders. — Anwendbares Datenschutzrecht bei Internet-Diensteanbietern, ZD 2013, S. 371-375

Ders. — Die Renaissance des Verbotsprinzips im Datenschutz, DuD 2013, S. 75-79

Ders. / Kühn, Ulrich — Datenschutzrechtlicher Rahmen für „Device Fingerprinting“ – Das klammheimliche Ende der Anonymität im Internet?, ZD 2014, S. 285-290

Kartheuser, Ingemar / Klar, Manuel — Wirksamkeitskontrolle von Einwilligungen auf Webseiten – Anwendbares Recht und inhaltliche Anforderungen im Rahmen gerichtlicher Überprüfungen , ZD 2014, S. 500-505

Klar, Manuel	Privatsphäre und Datenschutz in Zeiten technischen und legislativen Umbruchs, DÖV 2013, S. 103-113
Ders.	Räumliche Anwendbarkeit des (europäischen) Datenschutzrechts – Ein Vergleich am Beispiel von Satelliten-, Luft- und Panoramastraßenaufnahmen, ZD 2013, S. 109-115
Keppeler, Lutz Martin	Was bleibt vom TMG-Datenschutz nach der DS-GVO? Lösung und Schaffung von Abgrenzungsproblemen im Multimedia-Datenschutz, MMR 2015, S. 779-783
Kipker, Dennis-Kenji / Voskamp, Frederike	Datenschutz in sozialen Netzwerken nach der Datenschutzgrundverordnung, DuD 2012, S. 737-742
Ders.	Informationelle Freiheit und staatliche Sicherheit – rechtliche Herausforderungen moderner Überwachungstechnologien, 1. Auflage, Tübingen 2016
Kosinski, Michael / Stillwell, David/ Graepel, Thore	Private traits and attributes are predictable from digital records of human behavior, PNAS 2013, 110 (15), S. 5802-5805, vgl. auch http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html
Koós, Clemens	Das Vorhaben eines einheitlichen Datenschutzes in Europa – Aktueller Stand des europäischen Gesetzgebungsverfahrens, ZD 2014, S. 9-15
Ders. / Englisch, Bastian	Eine „neue“ Auftragsdatenverarbeitung? – Gegenüberstellung der aktuellen Rechtslage und der DS-GVO in der Fassung des LIBE-Entwurfs, ZD 2014, S. 276-285
Köhler, Helmut / Bornkamm, Joachim (Hrsg.)	Beck’sche Kurzkommentare, Gesetz gegen den unlauteren Wettbewerb, 33. Auflage, München 2015 (zitiert: *Bearbeiter*, in: *Köhler/Bornkamm*, UWG)
Köpernik, Kristin	Zur Notwendigkeit einer Verbandsklage bei Datenschutzverstößen, VuR 2014, S. 240-243
Kötter, Matthias / Nolte, Jakob	Was bleibt von der „Polizeifestigkeit des Versammlungsrechts“?, DÖV 2009, S. 399-406
Kremer, Sascha	Datenschutz bei Entwicklung und Nutzung von Apps für Smart-Devices, CR 2012, S. 438-446

Ders. / Buchalik, Barbara	Zum anwendbaren Recht im internationalen Geschäftsverkehr – Internationales Privatrecht und rechtliche Vorgaben in Deutschland in der Korrektur von LG Berlin, Urt. v. 30.4.2013 – 15 O 02/12, CR 2013, S. 789-794
Ders.	Datenschutzerklärungen von Social Media Diensten: Anwendbares Recht und AGB-Kontrolle, RDV 2014, S. 73-83
Krohm, Niklas / Müller-Peltzer, Philipp	Wunsch nach Identifizierung anonymer Nutzer – Spannungsverhältnis von Kommunikationsfreiheit und Persönlichkeitsrechten, ZD 2015, S. 409-415
Kroschwald, Steffen	Kollektive Verantwortung für Datenschutz in der Cloud – Datenschutzrechtliche Folgen einer geteilten Verantwortlichkeit beim Cloud Computing, ZD 2013, S. 388-394
Krüger, Stefan / Maucher, Svenja-Ariane	Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis, MMR 2011, S. 433-439
Krüger, Wolfgang / Rauscher, Thomas (Hrsg.)	Münchner Kommentar zur Zivilprozessordnung, Band 3 Internationales und Europäisches Zivilprozessrecht, 4. Auflage, München 2013 (zitiert als: *Bearbeiter*, in: MüKo ZPO, Bd. 3)
Kutscha, Martin / Thomé, Sarah	Grundrechtsschutz im Internet?, 1. Auflage, Baden-Baden 2013
Kühling, Jürgen / Sivridis, Anastasios / Schwuchow, Mathis / Burghardt, Thorben	Das datenschutzrechtliche Vollzugsdefizit im Bereich der Telemedien – ein Schreckensbericht, DuD 2009, S. 335-342
Kühling, Jürgen	Datenschutz gegenüber öffentlichen Stellen im digitalen Zeitalter, Die Verwaltung (44) 2011, S. 525-562
Ders.	Rückkehr des Rechts: Verpflichtung von „Google & Co“ zu Datenschutz, EuZW 2014, S. 527-532
Ders. / Martini, Mario	Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW 2016, S. 448-454
Ladeur, Karl Heinz	Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken, DuD (24) 2000, S. 12-19

Larenz, Karl / Canaris, Claus-Wilhelm	Methodenlehre der Rechtswissenschaft, 3. Auflage, Berlin/Heidelberg 1995
Lauber-Rönsberg, Anne	Rechtsdurchsetzung bei Persönlichkeitsverletzungen im Internet: Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen, MMR 2014, S. 10-14
Lerch, Hana/ Krause, Beate/Hotho, Andreas/ Roßnagel, Alexander/ Stumme, Gerd	Social Bookmarking-Systeme – die unerkannten Datensammler – Ungewollte personenbezogene Datenverarbeitung?, MMR 2010, S. 454-458
von Lewinsky, Kai	Die Matrix des Datenschutzes – Besichtigung und Ordnung eines Begriffsfeldes, 1. Auflage, Tübingen 2014
Lichtnecker, Florian	Die Werbung in sozialen Netzwerken und mögliche hierbei auftretende Probleme, GRUR 2013, S. 135-140
Lindner, Eric	Die datenschutzrechtliche Einwilligung nach §§ 4 Abs. 1, 4a BDSG – ein zukunftsfähiges Institut?, 1. Auflage, Hamburg 2013 (zitiert: *Lindner*, Datenschutzrechtliche Einwilligung)
Lisken, Hans / Erhard, Denninger (Begr.)	Handbuch des Polizeirechts, *Denninger / Rachor* (Hrsg.), 5. Auflage, München 2012 (zitiert als: *Bearbeiter*, in: Handbuch des Polizeirechts)
Lorenz, Bernd	Anonymität im Internet? – Zur Abgrenzung von Diensteanbietern und Nutzern, VuR 2014, S. 83-90
Maisch, Michael Marc	Informationelle Selbstbestimmung in Netzwerken – Rechtsrahmen, Gefährderungslagen und Schutzkonzepte am Beispiel von Cloud Computing und Facebook, 1. Auflage, Berlin 2015 (zitiert: *Maisch*, Informationelle Selbstbestimmung)
Mantz, Reto	Störerhaftung für Datenschutzverstöße Dritter – Sperre durch DS-RL und DS-GVO? ZD 2014, S. 62-66
Martini, Mario / Fritzsche, Saskia	Zwischen Öffentlichkeitsauftrag und Gesetzesbindung: zum Dilemma deutscher Behörden bei der Einbindung privater Social-Media-Werkzeuge und Geodatendienste in ihre Internetangebote, VerwArch (104) 2013, S. 450-485
Ders.	Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl. 2014, S. 1481-1489

Ders. / Fritzsche, Saskia — Mitverantwortung in sozialen Netzwerken – Facebook-Fanpage-Betreiber in der datenschutzrechtlichen Grauzone, NVwZ-Extra (21) 2015, S. 1-16

Ders. — Wie neugierig darf der Staat im Cyberspace sein? Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen, VerwArch (107) 2016, S. 307-358

Masing, Johannes — Herausforderungen des Datenschutzes, NJW 2012, S. 2305-2311

Ders. — Vorläufige Einschätzung der „Google-Entscheidung des EuGH", Verfassungsblog 8/14, http://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/

Maunz, Theodor / Dürig, Günther (Begr.) — Grundgesetz Kommentar, *Herzog* u.a. (Hrsg.), Band 1, 73. Ergänzungslieferung, Stand Dezember 2014, München

(zitiert als: *Autor*, in: Maunz/Dürig, GG)

Mayer-Schönberger, Viktor — Die Tugend des Vergessens in digitalen Zeiten, 3. Auflage, Berlin 2015; aus dem Englischen übersetzt von Andrea Kamphuis (die englische Originalausgabe erschien 2009 unter dem Titel *Delete. The Virtue of Forgetting in the Digital Age*)

(zitiert als: *Mayer-Schönberger*, Die Tugend des Vergessens)

Ders. — Informationsrecht als Gestaltungsaufgabe: Eine transatlantische Begegnung, in: *Schweizer/Burkert/Grasser* (Hrsg.), Festschrift für Jean Nicolas Druey zum 65. Geburtstag, 1. Auflage, Zürich u.a. 2012

Moser-Knierim, Antonie — „Facebook-Login" – datenschutzkonformer Einsatz möglich? – Einsatz von Social PlugIns bei Authentifizierungsdiensten, ZD 2013, S. 263-266

Nebel, Maxi / Richter, Philipp — Datenschutz bei Internetdiensten nach der DS-GVO – Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf, ZD 2012, S. 407-413

Dies. — Facebook knows your vote! – Big Data und der Schutz politischer Meinungen in sozialen Netzwerken, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, 1. Auflage, Baden-Baden 2015, S. 89-110

Dies. — Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht, ZD 2015, S. 517-522

Neuberger, Christoph / Gehrau, Volker (Hrsg.) — Soziale Netzwerke im Internet, in: StudiVZ – Diffusion, Nutzung und Wirkung eines sozialen Netzwerks im Internet, 1. Auflage, Heidelberg 2011

(zitiert als: *Neuberger*, in: Neuberger/Gehrau (Hrsg.), Soziale Netzwerke)

Neumann-Braun, Klaus / Autenrieth, Ulla P. (Hrsg.) — Freundschaft und Gemeinschaft im Social Web – Bildbezogenes Handeln und Peergroup-Kommunikation auf Facebook & Co, 1. Auflage, Baden-Baden 2011 (zitiert als: *Autor*, in: Freundschaft und Gemeinschaft im Social Web (Neumann-Braun/Autenrieth (Hrsg.))

Newman, Nathan — The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google, 40 William Mitchell L. Rev., 2013-2014, S. 849-889

Nguyen, Alexander — Die zukünftige Datenschutzaufsicht in Europa – Anregungen für den Trilog zu Kap. VI bis VII der DS-GVO, ZD 2015, S. 265-270

Niemann, Fabian/ Paul, Jörg-Alexander — Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computings, K&R 2009, S. 444-452

Nietsch, Thomas — Anonymität und die Durchsetzung urheberrechtlicher Ansprüche im Internet – Grundrechtliche Positionen im Spannungsfeld, 1. Auflage, Tübingen 2014 (zitiert als: *Nietsch*, Anonymität)

Nolte, Norbert — Zum Recht auf Vergessen im Internet – Von digitalen Radiergummis und anderen Instrumenten, ZRP 2011, S. 236-240

Ders. — Das Recht auf Vergessenwerden – mehr als nur ein Hype?, NJW 2014, S. 2238-2242

Oermann, Markus — Das „Kommunikationspanopticum" als Herausforderung für Datenschutzregulierung von inkludierenden Onlinekommunikations-diensten, In: *Taeger* (Hrsg.) Law as a Service, Recht im Internet und Cloudzeitalter, Band 1, DSRI-Tagungsband, 1. Auflage, Edewecht 2013, S. 53-68

Ders. / Staben, Julian — Mittelbare Grundrechtseingriffe durch Abschreckung? – Zur grundrechtlichen Bewertung polizeilicher „Online-Streifen" und „Online-Ermittlungen" in sozialen Netzwerken, Der Staat (52) 2013, S. 630-660

Ohly, Ansgar — Die Verantwortlichkeit von Intermediären, ZUM 2015, S. 308-318

Pahlen-Brandt, Ingrid — Zur Personenbezogenheit von IP-Adressen, K&R 2008, S. 288-290

Pariser, Eli — The Filter Bubble – What the Internet is Hiding from You, London 2011, (zitiert als: *Pariser*, Filter Bubble)

Pauly, Daniel / Ritzer, Christoph / Geppert, Nadine	Gilt europäisches Datenschutzrecht auch für Niederlassungen ohne Datenverarbeitung? Weitrechende Folgen für internationale Konzerne, ZD 2013, S. 423-425
Peifer, Karl-Nikolaus	Verhaltensorientierte Nutzeransprache – Tod durch Datenschutz oder Moderation durch das Recht?, K&R 2011, S. 543-547
Ders.	Konvergenz in der Störer- und Verbreiterhaftung – Vom Störer zum Verbreiter?, AfP 2014, S. 18-23
Pernice, Ingolf	Das europäische Verwaltungsrecht in der Konsolidierungsphase, Die Verwaltung (44) 2011, S. 577-599
Petri, Thomas	Déjà vu – datenschutzpolitische Aufarbeitung der PRISM-Affäre; Appell nach mehr Transparenz der nachrichtendienstlichen Tätigkeit, ZD 2013, S. 557-561.
Ders.	Datenschutzrechtliche Verantwortlichkeit im Internet – Überblick und Bewertung der aktuellen Rechtsprechung, ZD 2015, S. 103-106
Ders.	Auftragsdatenverarbeitung – heute und morgen; Reformüberlegungen zur Neuordnung des Europäischen Datenschutzrechts, ZD 2015, S. 305-309
Pieroth, Bodo / Schlink, Bernhard / Kniesel, Michael (Begr.)	Polizei- und Ordnungsrecht mit Versammlungsrecht, *Kingreen / Poscher* (Hrsg.), 8. Auflage, München 2014
Pießkalla, Michael	Zur Reichweite der Impressumspflicht in sozialen Netzwerken, ZUM 2014, S. 368-374
Piltz, Carlo	Der Like-Button von Facebook – Aus datenschutzrechtlicher Sicht: „Gefällt mir nicht!“, CR 2011, S. 657-664
Ders.	Rechtswahlfreiheit im Datenschutzrecht, K & R 2012, S. 640-645
Ders.	Soziale Netzwerke im Internet – Eine Gefahr für das Persönlichkeitsrecht? 1. Auflage, Frankfurt a.M. 2013
Ders.	Störerhaftung im Datenschutzrecht?, K&R 2014, S. 80-85
Plath, Kai-Uwe (Hrsg.)	Kommentar zum BDSG und zur DS-GVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. Auflage, Köln 2016 (zitiert als: *Bearbeiter*, in: Plath, BDSG)
Plog, Philipp	Zur Zulässigkeit eines Bewertungsportals für Lehrer (spickmich.de), zugleich Anmerkung zu LG Köln v. 11.7.2007, Az. 28 O 263/07, CR 2007, S. 668-670

Pohle, Jan/ Ammann, Thorsten — Über den Wolken… – Chancen und Risiken des Cloud Computing, CR 2009, S. 273-278

Polenz, Sven — Die Datenverarbeitung durch Facebook auf dem Prüfstand, VuR 2012, S. 207-213

Raabe, Oliver / Lorenz, Mieke — Die datenschutzrechtliche Einwilligung im Internet der Dienste – Zur Notwendigkeit qualifizierter elektronischer Signaturen, DuD 2011, S. 279-284

Radlanski, Philip — Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 1. Auflage, Tübingen 2016

(zitiert als: *Radlanski*, Das Konzept der Einwilligung)

Redeker, Helmut — IT-Recht, 5. Auflage, München 2012

Richter, Philipp — Die Wahl ist geheim… so what?, DÖV 2013, S. 961-970

Ders. — Ein anonymes Impressum? Profile in sozialen Netzwerken zwischen Anbieterkennzeichnung und Datenschutz, MMR 2014, S. 517-521

Ders. — Big Data und demokratische Willensbildung aus verfassungsrechtlicher Sicht, in: ders. (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, 1. Auflage, Baden-Baden 2015, S. 45-67

Riefa, Christine / Markou, Christiana — Online marketing: advertisers know you are a dog on the Internet!, in: *Savin/Trzaskowski* (Hrsg.), Research Handbook on EU Internet Law, 1. Auflage, Cheltenham 2014, S. 383-410

Rockstroh, Sebastian — Impressumspflicht auf Facebook-Seiten – Wann werden Telemedien „in der Regel gegen Entgelt" angeboten?, MMR 2013, S. 627-630

Rogall-Grothe, Cornelia — Ein neues Datenschutzrecht für Europa, ZRP 2012, S. 193-196

Rogosch, Patricia Maria — Die Einwilligung im Datenschutzrecht, 1. Auflage, Baden-Baden 2013

Rosengarten, Carsten/ Römer, Sebastian — Der „virtuelle verdeckte Ermittler" in sozialen Netzwerken und Internetboards, NJW 2012, S. 1764-1768

Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen — Modernisierung des Datenschutzrechts – Gutachten im Auftrag des Bundesministeriums des Inneren, Berlin 2001

Roßnagel, Alexander (Hrsg.) Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, 1. Auflage, München 2003

(zitiert: *Autor*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht)

Ders. (Hrsg.) Recht der Multimedia-Dienste – Kommentar zum IuKDG und MDStV, Stand: 7. Ergänzungslieferung, April 2005, München

(zitiert als: *Autor*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste)

Ders. Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, S. 71-75

Ders. Persönlichkeitsentfaltung zwischen Eigenverantwortung, gesellschaftlicher Selbstregulierung und staatlicher Regulierung, in: *Bieber/Eifert/Groß/Lamla* (Hrsg.), Soziale Netze in der digitalen Welt – Das Internet zwischen egalitärer Teilhabe und ökonomischer Macht, 1. Auflage Frankfurt a.M. 2009, S. 271-285 (zitiert als: *Roßnagel*, Persönlichkeitsentfaltung, in: Bieber/Eifert (u.a.) (Hrsg.), Soziale Netze in der digitalen Welt)

Ders. / Hornung, Gerrit Ein Ausweis für das Internet – Der neue Personalausweis enthält einen „elektronischen Identitätsnachweis“, DÖV 2009, S. 301-306

Ders. / Richter, Philipp / Nebel, Maxi Besserer Internetdatenschutz für Europa – Vorschläge zur Spezifizierung der DS-GVO, ZD 2013, S. 103-108

Ders. / Kroschwald, Steffen Was wird aus der Datenschutzgrundverordnung?, ZD 2014, S. 495-500

Ders. / Nebel, Maxi / Richter, Philipp Was bleibt vom europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, S. 455-461

Ders. (Hrsg.) Europäische Datenschutz-Grundverordnung; Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, 1. Auflage, Baden-Baden 2017

(zitiert als: *Autor*, in: Roßnagel (Hrsg.), Europäische DS-GVO)

Sandfuchs, Barbara Privatheit wider Willen? Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischem Verfassungsrecht, 1. Auflage, Baden-Baden 2016

Säcker, Franz Jürgen (u.a.) (Hrsg.) Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 7. Auflage, München 2015

(zitiert als: *Bearbeiter*, in: MüKo BGB, Bd. 1)

Ders. (u.a.) (Hrsg.)	Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 3, 7. Auflage, München 2016 (zitiert als: *Bearbeiter*, in: MüKo BGB, Bd. 3)
Ders. (u.a.) (Hrsg.)	Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, 6. Auflage, München 2013 (zitiert als: *Bearbeiter*, in: MüKo BGB, Bd. 6)
Schaar, Peter	Neue Konzeptionen für den Datenschutz, in: *Vieweg/Gerhäuser* (Hrsg.), Digitale Daten in Systemen und Geräten, 1. Auflage, Köln 2010
Schaarschmidt, Theodor	Die Brandstifter aus dem Netz – Gehirn & Geist, Spektrum der Wissenschaft, 5/2016, S. 30-36.
Schantz, Peter	Die Datenschutzgrundverordnung – Beginn einer neuen Zeitrechnung im Datenschutz, NJW 2016, S. 1841-1847
Schapiro, Leo	Unterlassungsansprüche gegen die Betreiber von Internet-Auktionshäusern und Internet-Meinungsforen, 1. Auflage, Tübingen 2011 (zitiert als: *Schapiro*, Unterlassungsansprüche)
Schenk, Michael/ Niemann, Julia/ Reinmann, Gabi/ Roßnagel, Alexander (Hrsg.)	Digitale Privatsphäre: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen, 1. Auflage, Düsseldorf 2012 (zitiert als: *Autor*, in: Schenk u.a. (Hrsg.), Digitale Privatsphäre)
Schenke, Wolf-Rüdiger	Polizei- und Ordnungsrecht, 9. Auflage Heidelberg (u.a.) 2016
Schleipfer, Stefan	Datenschutzkonformes Webtracking nach Wegfall des TMG – Was bringen die DS-GVO und die ePrivacy-Verordnung?, ZD 2017, S. 460 466.
Schliesky, Urs / Hoffmann, Christian/ Luch, Anika / Schulz, Sönke / Borchers, Corinna	Schutzpflichten und Drittwirkung im Internet – Das Grundgesetz im digitalen Zeitalter, 1. Auflage, Baden-Baden 2014
Schnabel, Christoph / Freund, Bernhard	„Ach wie gut, dass niemand weiß…" – Selbstdatenschutz bei der Nutzung von Telemedienangeboten, CR 2010, S. 718-721
Schneider, Hartmut (Hrsg.)	Münchner Kommentar zur Strafprozessordnung, Band 2, §§ 151-332 StPO, 1. Auflage, München 2016 (zitiert als: *Bearbeiter*, in: Müko-StPO, Bd. 2)

Schneider, Jens-Peter — Stand und Perspektiven des Europäischen Datenverkehrs- und Datenschutzrechts, in: Die Verwaltung (44) 2011, S. 499-524

Schneider, Jochen / Härting, Niko — Warum wir ein neues BDSG brauchen – Kritischer Beitrag zum BDSG und dessen Defiziten, ZD 2011, S. 63-68

Schneider, Matthias — WhatsApp & Co. – Dilemma um anwendbare Datenschutzregeln; Problemstellung und Regelungsbedarf bei Smartphone-Messengern, ZD 2014, S. 231-237

Schoch, Friedrich — Der Zweckveranlasser im Gefahrenabwehrrecht, Jura 2009, S. 360-366

Schreiber, Kristina / Kohm, Simon — Rechtssicherer Datentransfer unter dem EU-US-Privacy-Shield? Der transatlantische Datentransfer in der Unternehmenspraxis, ZD 2016, S. 255-260

Schröder, Birgit / Hawxwell, Anne / Münzing, Heike — Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages, und Social-PlugIns; Ausarbeitung des wissenschaftlichen Dienstes des Bundestages, Fassung vom 7. Oktober 2011, Az. WD 3 – 3000 – 306/11 neu

(zitiert als: *Schröder/Hawxwell*, Verletzung datenschutzrechtlicher Bestimmungen, in Wissenschaftlicher Dienst des BT)

Schulz, Sönke E. — Cloud Computing in der öffentlichen Verwaltung: Chancen – Risiken – Modelle, MMR 2010, S. 75-80

Ders./ Hoffmann, Christian — Grundrechtsrelevanz staatlicher Beobachtung im Internet – Internet-Streifen der Behörden und das „Autorisierungskonzept" des BVerfG, CR 2010, S. 131-136

Ders. / Ders. — Praxis der Kommunalverwaltung – Soziale Medien in der öffentlichen Verwaltung, Band L 16 Bund, Stand Oktober 2013

(zitiert als: *Schulz/Hoffmann*, in: PdK, Band L 16 Bund)

Ders. — Datenschutz als überindividuelles Interesse? – Anmerkungen zur geplanten Reform des UKlaG, ZD 2014, S. 510-514

Schwartmann, Rolf / Theodoru, Elissavet — Aktuelle Rechtsprechung des EuGH zum Datenschutzrecht, RDV 2014, S. 61-72

Schwartmann, Rolf — Verantwortlichkeit Sozialer Netzwerke nach dem Netzwerkdurchsetzungsgesetz, GRUR-Prax 2017, S. 317-319

Simitis, Spiros (Hrsg.)	Bundesdatenschutzgesetz Kommentar, 8. Auflage, Baden-Baden 2014 (zitiert als: *Bearbeiter*, in: Simitis, BDSG)
Simo, Hervais	Big Data: Opportunities and Privacy Challenges, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, 1. Auflage, Baden-Baden 2015, S. 13-44
Singelnstein, Tobias	Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, S. 593-606
Skouris, Vassilios	Leitlinien der Rechtsprechung des EuGH zum Datenschutz, NVwZ 2016, S. 1359-1364
Slobogin, Christopher	Die Zukunft des Datenschutzes in den USA, Die Verwaltung (44) 2011, S. 465-497
Soiné, Michael	Personale verdeckte Ermittlungen in sozialen Netzwerken zur Strafverfolgung, NStZ 2014, S. 248-252
Spieker gen. Döhmann, Indra	Die Durchsetzung datenschutzrechtlicher Mindestanforderungen bei Facebook und anderen sozialen Netzwerken – Überlegungen zu Vollzugsdefiziten im Datenschutzrecht, K&R 2012, S. 717-725
Dies.	Verantwortung bei begrenztem Wissen in der digitalen Welt, in: Fehling/Schliesky, zusammen mit dem Deutschen Institut für Vertrauen und Sicherheit im Internet (Hrsg.), S. 53-72, Baden-Baden – *Erscheinen in Vorbereitung*
Spindler, Gerald/	Recht der elektronischen Medien, 3. Auflage, München 2015
Schuster, Fabian (Hrsg.)	(zitiert als: *Bearbeiter*, in: Spindler/Schuster)
Spindler, Gerald	Persönlichkeitsrecht und Datenschutz im Internet – Anforderungen und Grenzen einer Regulierung, Gutachten F zum 69. Deutschen Juristentag, Band I, München 2012. (zitiert als: *Spindler*, Gutachten F zum 69. dt. Juristentag, 2012)
Ders.	Die Störerhaftung im Internet – (k)ein Ende in Sicht? Geklärte und ungeklärte Fragen, in: *Alexander/Bornkamm* (Hrsg.), Festschrift für Helmut Köhler zum 70. Geburtstag, 1. Auflage, München 2014, S. 695-713 (zitiert als: Spindler, Störerhaftung im Internet, in: FS Köhler (Alexander u.a., Hrsg.), S. 696 ff.)

Ders.	Durchbruch für ein Recht auf Vergessen(werden)? – Die Entscheidung des EuGH in Sachen Google Spain und ihre Auswirkungen auf das Datenschutz- und Zivilrecht, JZ 2014, S. 981-991
Ders.	Datenschutz- und Persönlichkeitsrechte im Internet: Der Rahmen für Forschungsaufgaben und Reformbedarf, GRUR Beilage 2014, S. 101-108
Ders.	Verbandsklagen und Datenschutz – das neue Verbandsklagerecht: Neuregelungen und Probleme, ZD 2016, S. 114-119
Ders.	Das neue Telemediengesetz – WLAN-Störerhaftung endgültig adé?, NJW 2017, S. 2305-2308
Stadler, Thomas	Verstoßen Facebok und Google Plus gegen deutsches Recht? Ausschluss von Pseudonymen auf Social-Media-Plattformen, ZD 2011, S. 57-59
Steinrötter, Björn	Kollisionsrechtliche Bewertung der Datenschutzrichtlinien von IT-Dienstleistern, MMR 2013, S. 691-694
Stelkens, Paul / Bonk, Heinz Joachim / Sachs, Michael (Hrsg.)	Verwaltungsverfahrensgesetz Kommentar, 8. Auflage, München 2014 (zitiert als: *Bearbeiter*, in: Stelkens/Bonk/Sachs, VwVfG)
Strahilevitz, Lior Jacob	Toward a Positive Theory of Privacy Law, 126 Harv. L. Rev., 2012-2013, S. 2010-2042
Sydow, Gernot / Kring, Markus	Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug, ZD 2014, S. 271-276
Taeger, Jürgen/ Gabel, Detlev (Hrsg.)	Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage, Frankfurt a.M. 2013 (zitiert als: *Bearbeiter*, in: Taeger/Gabel, BDSG)
Tettinger, Peter / Ergbuth, Wilfried / Mann, Thomas	Besonders Verwaltungsrecht – Kommunalrecht, Polizei- und Ordnungsrecht, Baurecht, 11. Auflage, Heidelberg u.a. 2012
Thaler, Richard / Sunstein, Cass	Nudge – Wie man kluge Entscheidungen anstößt, 4. Auflage, Berlin 2009 (zitiert als: *Thaler/Sunstein*, Nudge)
Thoma, Florian	Risiko im Datenschutz – Stellenwert eines systematischen Risikomangements in BDSG und DS-GVO-E, ZD 2013, S. 578-581

Uerpmann-Wittzack, Robert/ Jankowska-Gilberg, Magdalena	Die europäische Menschenrechtskonvention als Ordnungsrahmen für das Internet, MMR 2008, S. 83-89
Veil, Winfried	DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip, ZD 2015, S. 347-353
Voigt, Paul / Alich, Stefan	Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber, NJW 2011, S. 3541-3544
Voigt, Paul	Webbrowser Fingerprints – Tracking ohne IP-Adressen und Cookies? In: *Taeger* (Hrsg.) Law as a Service, Recht im Internet und Cloudzeitalter, Band 1, 1. Auflage, DSRI-Tagungsband, Edewecht 2013, S. 157-172 (zitiert als: Voigt, Webbrowser Fingerprints, in: LaaS, Recht im Internet und Cloudzeitalter (Taeger (Hrsg.))
Ders.	Internationale Anwendbarkeit des deutschen Datenschutzrechts, ZD 2014, S. 15-21
Ders.	Der Vorrang der Datenschutzrichtlinie vor nationalem Recht, K&R 2014, S. 325-327
Volkmann, Uwe	Polizeirecht als Sozialtechnologie, NVwZ 2009, S. 216-222
von der Groeben, Hans / Schwarze, Jürgen / Hatje, Armin	Europäisches Unionsrecht – EUV, AEUV, GrCH – Nomos Kommentar, 7. Auflage, Baden-Baden 2015 (zitiert als: *Bearbeiter*, in: von der Groeben/Schwarze/Hatje (Hrsg.))
von der Lühe, Ulrike	Die sozialen Netzwerke aus Sicht der betroffenen Akteure: Die Perspektive der Nutzer, in: *Hill/Martini/Wagner* (Hrsg.), Facebook, Google & Co – Chancen und Risiken, 1. Auflage, Baden-Baden 2013, S. 69-72
Voßkuhle, Andreas	Neue Verwaltungsrechtswissenschaft, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, § 1, 2. Auflage, München 2012
Wagner, Axel-Michael/ Blaufuß, Henning	Datenexport als juristische Herausforderung: Cloud Computing, BB 2012, S. 1751-1755
Wauters, Ellen / Lievens, Eva / Valcke, Peggy	Towards a better protection of social media users: a legal perspective on the terms of use of social networking sites, International Journal of Law and Information Technology, 2014 (22), S. 254-294

Weichert, Thilo — Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, S. 1463-1469

Ders. — Facebook, der Datenschutz und die öffentliche Sicherheit, in: *Möllers/van Ooyen* (Hrsg.), Jahrbuch Öffentliche Sicherheit 2012/2013, Frankfurt a.M. 2013, S. 379-391

(zitiert: *Weichert*, JBÖS 2012/2013)

Ders. — Big Data und Datenschutz, ZD 2013, S. 251-259

Ders. — Informationstechnische Arbeitsteilung und datenschutzrechtliche Verantwortung – Plädoyer für eine Mitverantwortlichkeit bei der Verarbeitung von Nutzungsdaten, ZD 2014, S. 605-610

Ders. — EU-US-Privacy-Shield – Ist der transatlantische Datentransfer nun grundrechtskonform? Eine erste Bestandsaufnahme, ZD 2016, S. 209-217

Weidlich-Flatten, Eva — Verbraucherschutzverbände als Heilsbringer für den Datenschutz? ZRP 2014, S. 196-198

Whitman, James Q. — The two Western Cultures of Privacy: Dignity versus Liberty, in: Yale Law Journal (113) 2004, S. 1151-1221

Wieber, Andreas — Datenschutz in sozialen Netzwerken, in: *Kaal u.a.* (Hrsg.), Festschrift zu Ehren von Christian Kirchner: Recht im ökonomischen Kontext, Festschrift anlässlich seines 70. Geburtstages, 1. Auflage, Tübingen 2014, S. 423-439

(zitiert als: *Wieber*, Datenschutz in sozialen Netzwerken, in: FS Kirchner)

Wolff, Heinrich Amadeus / Brink, Stefan — Datenschutzrecht in Bund und Ländern – Grundlagen, Bereichsspezifischer Datenschutz, BDSG – Kommentar, 1. Auflage, München 2013

Wolff, Johanna — Eine Annährung an das Nudge-Konzept nach Richard H. Thaler und Cass R. Sunstein aus rechtswissenschaftlicher Sicht, RW 2015, S. 194-222

v. Zimmermann, Georg — Die Einwilligung im Internet, 1. Auflage, Berlin 2014

Anhang 2: Internetquellen

Alle aus dem Internet entnommenen Quellen wurden – soweit nicht explizit anders vermerkt – zuletzt aufgerufen am 3. Januar 2018. Bei Nutzungsvereinbarungen und Ähnlichem ist aus Klarstellungsgründen zusätzlich der Stand der letzten Aktualisierung durch die Verwender vermerkt.

AK I „Staatsrecht und Verwaltung“	Ergebnisbericht der Arbeitsgruppe des AK I „Staatsrecht und Verwaltung“ zum Datenschutz in Sozialen Netzwerken vom 4. April 2012, https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf
AK Vorratsdaten-speicherung	„Keine NSA für alle - Internetüberwachung durch Privatpersonen vorläufig abgewendet“, Pressemitteilung vom 14.12.2015 http://www.vorratsdatenspeicherung.de/content/view/766/79/lang,de/
Bayrischer Beauftragter für Datenschutz	Der Bayerische Landesbeauftragte für den Datenschutz informiert zum Thema: Soziale Netzwerke – Fanpages bayerischer öffentlicher Stellen in sozialen Netzwerken zum Zweck der Öffentlichkeitsarbeit, v. 28.3.2013 https://www.datenschutz-bayern.de/technik/orient/oh_fanpages.pdf
Belgian Commission fort he Protection of Privacy	Recommendation no. 04/2015 of 13 May 2015, relating to Facebook et al. https://www.privacycommission.be/sites/privacycommission/files/documents/recommendation_04_2015_0.pdf
Bitkom	Soziale Netzwerke – dritte, erweiterte Studie, https://www.bitkom.org/Publikationen/2013/Studien/Soziale-Netzwerke-dritte-erweiterte-Studie/SozialeNetzwerke-2013.pdf
BuiltWith	http://trends.builtwith.com/widgets/Facebook-Like
Bundeskartellamt	Bundeskartellamt eröffnet Verfahren gegen Facebook wegen Verdachts auf Marktmachtmissbrauch durch Datenschutzverstöße, http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568
Bundeskartellamt	Vorläufige Einschätzung im Facebook-Verfahren: Das Sammeln und Verwerten von Daten aus Drittquellen außerhalb der Facebook Website ist missbräuchlich http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2017/19_12_2017_Facebook.pdf?__blob=publicationFile&v=3

CNN (Sifry, Micah)	How Obama's data-crunching prowess may get him re-elected, http://edition.cnn.com/2011/10/09/tech/innovation/obama-data-crunching-election/index.html
Das, Sauvik / Kramer, Adam	Self-Censorhip on Facebook, in: AAAI Publications, Seventh International AAAI Conference on Weblogs and Social Media, 2013, S. 120-127 http://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350
Düsseldorfer Kreis	Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 8.12.2011; Datenschutz in sozialen Netzwerken http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.pdf?__blob=publicationFile&v=1
Europe vs. Facebook	Mini-Update: Irish High Court: Data Protection Commissioner to investigate "Facebook" over NSA spy program http://www.europe-v-facebook.org/MU_HC.pdf
Facebook	Nutzungsbedingungen, Stand 30. Januar 2015 https://www.facebook.com/legal/terms
Facebook	Datenrichtlinie, Stand 29. September 2016 https://www.facebook.com/privacy/explanation
Facebook	Cookie-Richtlinie, Stand 20. März 2017 https://www.facebook.com/policies/cookies/
Facebook Annual Reports 2013, 2014 und 2015	http://files.shareholder.com/downloads/AMDA-NJ5DZ/55276922x0x741493/EDBA9462-3E5E-4711-B0B4-1DFE9B541222/FB_AR_33501_FINAL.pdf https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB2014AR.pdf https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2015-Annual-Report.pdf
Facebook Quarterly Report Filed 10/30/14 for the Period Ending 09/30/14	http://investor.fb.com/secfiling.cfm?filingID=1326801-14-68&CIK=1326801 (zuletzt aufgerufen am 18.10.2016)
Facebook, Form 10-k für die amerikanische SEC, abgegeben für	https://www.sec.gov/Archives/edgar/data/1326801/000132680115000006/fb-12312014x10k.htm

die Zeiträume bis zum 31.12.2014 und 31.12.2015	https://www.sec.gov/Archives/edgar/data/1326801/000132680116000043/fb-12312015x10k.htm
Frankfurter Allgemeine Zeitung (Mathias Müller von Blumencron)	Was das Google Urteil bedeutet http://www.faz.net/aktuell/wirtschaft/unternehmen/eugh-urteil-ueber-google-recht-auf-vergessen-im-netz-12937165.html
Frankfurter Allgemeine Zeitung (Kafsack, Hendrik)	EU-Kommission will mehr Datenschutz – „Ein Recht auf Vergessen im Netz“, http://www.faz.net/aktuell/politik/europaeische-union/eu-kommission-will-mehr-datenschutz-ein-recht-auf-vergessen-im-netz-11623455.html
Google (/Alphabet) Financial Tables	https://investor.google.com/financial/tables.html
Handelsblatt – Kerkmann, Axel u.a.	Indien und Facebook.org - Indiens Aufstand gegen Mark Zuckerberg http://www.handelsblatt.com/unternehmen/it-medien/facebook-und-internet-org-indiens-aufstand-gegen-mark-zuckerberg/11663668-all.html
Heise Online (Holger Bleich)	http://www.heise.de/newsticker/meldung/Digitaler-Radiergummi-ist-gestartet-1175979.html
Heise Online (Andreas Wilkens)	https://www.heise.de/newsticker/meldung/Aigner-Hoechster-Datenschutz-made-in-Germany-1163613.html
Heise Online (Berger, Daniel)	Schützen und teilen – Social-Media-Buttons datenschutzkonform nutzen http://www.heise.de/ct/ausgabe/2014-26-Social-Media-Buttons-datenschutzkonform-nutzen-2463330.html
Heise Online	Belgisches Gericht: Facebook darf keine Daten von Nicht-Mitgliedern sammeln http://www.heise.de/newsticker/meldung/Belgisches-Gericht-Facebook-darf-keine-Daten-von-Nicht-Mitgliedern-sammeln-2912586.html
Horvát, Emőke-Ágnes / Hanselmann, Michael / Hamprecht, Fred. A. / Zweig, Katharina A.	One Plus One makes Three (for Social Networks), 2012, PLoS ONE, Volume 7, Issue 4: e34740. doi:10.1371/journal.pone.0034740 , http://www.plosone.org/
Irish Data Protection Commissioner	Facebook Ireland Ltd. – Report of Audit, 21 December 2011 https://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf

	Appendices to Facebook Ireland Audit Report, 21 December 2011 https://dataprotection.ie/documents/facebook%20report/final%20report/Appendices.pdf
	Facebook Ireland Ltd. – Report of Re-Audit, 21 September 2012, http://www.dataprotection.ie/documents/press/facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf
Interdisciplinary Center for Law and ICT and ICT/Centre for IP Rights der KU Leuven (Van Alsenoy, Brendan u.a.)	From social media service to advertising network – A critical Analysis of Facebook's Revised Polices, Entwurf 25. August 2015, Version 1.3 https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf
	KU Leuven Centre for IT & IP Law and iMinds-SMIT advise Belgian Privacy Commission in Facebook investigation http://www.law.kuleuven.be/icri/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation
	Facebook Tracking Through Social Plugins – Technical report prepared for the Belgian Privacy Commission, Version 1.1, 24. Juni 2015 https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf
Konferenz der Datenschutzbeauftragten des Bundes und der Länder	Orientierungshilfe „Soziale Netzwerke", Stand 14. März 2013 https://www.datenschutz-bayern.de/technik/orient/oh_soziale-netze.pdf
Lessig, Lawrence	Code is Law – On Liberty in Cyberspace, Harvard Magazine, January-February 2000, http://www.harvardmagazine.com/2000/01/code-is-law-html
Linked In	Nutzervereinbarung, Stand 7. Juni 2017 https://www.linkedin.com/legal/user-agreement?trk=uno-reg-guest-home-user-agreement
meinVZ	Allgemeine Geschäftsbedingungen für die Nutzung des Netzwerks, Version 2.0 http://www.meinvz.net/l/terms
MySpace	Myspace Services Terms of Use Agreement, Stand 27. April 2017

	https://myspace.com/pages/terms
Politico, (Romano, Lois)	Obama's data advantage http://www.politico.com/news/stories/0612/77213.html
Proksch & Fritzsche Frank Fletzberger Rechtsanwälte GmbH	Klageschrift im Verfahren Schrems v Facebook Ireland Ltd., Wien, vom 31.7.2014 vor dem Handelsgericht Wien http://www.europe-v-facebook.org/sk/sk.pdf
Projecter	Top 10 der deutschen Facebook Shops http://www.projecter.de/blog/social-media/top-10-der-deutschen-facebook-shops.html
Reuters Institute for the Study of Journalism; University of Oxford; Newman, Nic (u.a.)	Reuters Institute Digital News Report 2016, http://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital-News-Report-2016.pdf
Snapchat	Nutzungsbedingungen, Stand 26. September 2017 https://www.snap.com/de-DE/terms/#terms-row
Spiegel Online (Friedrich, Hans-Peter)	Informationelle Selbstbestimmung: Das "Recht auf Vergessen" und die Netzfreiheit, http://www.spiegel.de/netzwelt/netzpolitik/informationelle-selbstbestimmung-das-recht-auf-vergessen-und-die-netzfreiheit-a-817830.html
Statista	http://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/ http://de.statista.com/statistik/daten/studie/219718/umfrage/haeufigkeit-der-nutzung-von-ausgewaehlten-sozialen-netzwerken/
StudiVZ	Allgemeine Geschäftsbedingungen für die Nutzung von poolworks Ltd (www.studivz.net), Version 2.0 http://www.studivz.net/l/terms
Süddeutsche Zeitung (Javier Cáceres)	Facebooks Bank-Pläne alarmieren Datenschützer http://www.sueddeutsche.de/digital/lizenz-in-irland-beantragt-facebook-will-eine-bank-werden-1.1958655
Tencent Holdings Limited	Annual Report 2015, http://www.tencent.com/en-us/content/ir/news/2013/attachments/20131113.pdf (zuletzt aufgerufen am 18.10.2016)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)	Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, Stand 19. August 2011 https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf (zuletzt aufgerufen im Januar 2014)
Wikipedia	Soziales Netzwerk (Internet) https://de.wikipedia.org/wiki/Soziales_Netzwerk_(Internet)
Xing	Allgemeine Geschäftsbedingungen, Stand 1. April 2017 https://www.xing.com/terms
Zeit Online (Johannes Wendt)	Sie haben das Recht, von Google vergessen zu werden http://www.zeit.de/digital/datenschutz/2014-05/eugh-urteilt-ueber-recht-auf-vergessenwerden
Zeit Online (Patrick Beuth)	Wie Facebook mit Banken konkurrieren könnte http://www.zeit.de/digital/internet/2014-04/facebook-ueberweisungen-e-geld/komplettansicht
Zeit Online (Tai, Katharin)	Internet.org – Facebook oder nichts http://www.zeit.de/digital/internet/2015-04/internet-org-facebook-netzneutralitaet
Zeit Online (Stephan, Felix)	„Instant Articles“ – Die Privatisierung der Meinungsfreiheit http://www.zeit.de/kultur/2015-05/instant-articles-facebook-meinungsfreiheit/komplettansicht

Anhang 3: Stellungnahmen der Art. 29 Datenschutzgruppe

- Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, WP 163
- Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169
- Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, WP 171
- Stellungnahme 8/2010 zum anwendbaren Recht, WP 179
- Stellungnahme 15/2011 zur Definition der Einwilligung, WP 187
- Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht WP 194
- Stellungnahme 05/2012 zum Cloud Computing, WP 196
- Opinion 02/2013 on apps on smart devices, WP 202
- Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies, WP 208
- Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, WP 221
- Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP 224
- Joint Statement of the European data protection authorities assembled in the article 29 working, WP 227

Anhang 4: Rechtsprechungsverzeichnis

EuGH, Urt. v. 19.10.2016, Rs. C-582/14, *Breyer v. Deutschland* = NJW 2016, 3579 ff.

EuGH, Urt. v. 28.7.2016, Rs. C-191/15, *Verein für Konsumenteninformation v. Amazon EU* = EuZW 2016, 754 ff.

EuGH, Urt. v. 6.10.2015, Rs. C-362/14, *Schremms v. Data Protection Commisioner* = ZD 2015, 549 ff.

EuGH, Urt. v. 1.10.2015, Rs. C-230/14, *Weltimmo s.r.o.* = ZD 2015, 580 ff.

EuGH, Urt. v. 13.5.2014, Rs. C-131/12, *Google Spain* = JZ 2014, 1009 ff.

EuGH, Urt. v. 11.12.2014, Rs. C-212/13, *Frantisek Rynes* = EuZW 2015, 234 ff.

EuGH, Urt. v. 8.4.2014, Rs. C-293/12, C-594/12 = DVBl. 2014, 708 ff.

EuGH, Urt. v. 24.11.2011, Rs. C-468/10 und Rs. C-469/10, *ASNEF/FECEMD* = ZD 2012, 33 ff.

EuGH, Urteil vom 12. 7. 2011 - C-324/09, *L'Oréal/eBay u.a.* = GRUR 2011, 1025 ff.

EuGH, Urteil vom 23.03.2010 - C-236/08 bis C-238/08, *Google France SARL* / Louis Vuitton Malletier SA u.a. = NJW 2010, 2029 ff.

EuGH, Urt. v. 6.11.2003, Rs. C-101/01, *Lindqvist* = EuR 2004, 291 ff.

EuGH, Urt. v. 17.7.1997, Rs. C-190/95, *ARO Lease* = UR 1998, 185 ff.

EuGH, Urt. v. 4.7.1985, Rs. C-168/84, *Berkholz* = UR 1985, 226 ff.

BVerfG – Beschl. v. 16.6.2009, Az. 2 BvR 902/06 – Emailbeschlagnahme = DÖV 2009, 770

BVerfG – Urt. v. 11.3.2008, Az. 1 BvR 2074/05, 1254/07 – automatische Kennzeichenerfassung = BVerfGE 120, 378 ff.

BVerfG, Urt. v. 27.2. 2008, Az. 1 BvR 370, 595/07 – Onlinedurchsuchung = BVerfGE 120, 274 ff.

BVerfG, Beschl. v. 13.6.2007, Az. 1 BvR 1550/04, 2357/04, 603/05 = BVerfGE 118, 168 ff.

BVerfG, Urt. v. 13.2.2007, Az. 1 BvR 421/0 – Vaterschaftstest = BVerfGE 117, 202 ff.

BVerfG, Beschl. v. 23.10.2006, Az. 1 BvR 2027/02 – Schweigepflichtentbindung = BVerfGK 9, 353 ff.

BVerfG, Beschl. v. 4.4. 2006, Az. 1 BvR 518/02 – Rasterfahndung = BVerfGE 115, 320 ff.

BVerfG, Urt. v. 3. 3. 2004, Az. 1 BvR 2378/98, 1 BvR 1084/99 – Großer Lauschangriff = BVerfGE 109, 279 ff.

BVerfG, Beschl. v. 25.2.1999, Az. 1 BvR 1472–91 u.1510–91 = NJW 1999, 3404 ff.

BVerfG, Beschl. v. 14.8.1996, Az. 2 BvR 2088/93 = NJW 1996, 3146 ff.

BVerfG, Urt. v. 28.5.1993, Az. 2 BvF 2/90 und 4, 5/92 – Schwangerschaftsabbruch II = BVerfGE 88, 203 ff.

BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83 – Volkszählung = BVerfGE 65, 1 ff.

BVerfG, Urt. v. 15.1.1958, Az. 1 BvR 400/51 – Lüth = BVerfGE 7, 198 ff.

BGH, Urt. v. 16.5.2017, Az. VI ZR 135/13 = ZD 2017, 424 ff.

BGH, Urt. v. 15.2.2015, Az. I ZR 240/12 – Kinderhochstühle im Internet III = GRUR 2015, 485 ff.

BGH, Urt. v. 1.7.2014, Az. VI ZR 345/13 = BGHZ 201, 380 ff.

BGH, Beschl. v. 28.10.2014, Az.VI ZR 135/13 = ZD 2015, 80 ff.

BGH, Urt. v. 16. 5. 2013, Az. I ZR 216/11 – Kinderhochstühle im Internet II = GRUR 2013, 1229 ff.

BGH, Urt. v. 8. 5. 2012, Az. VI ZR 217/08 = NJW 2012, 2197 ff.

BGH, Urt. v. 19.4.2012, Az. I ZB 80/11 = NJW 2012, 2958 ff.

BGH, Urt. v. 25.10.2011, Az. VI ZR 93/10 = NJW 2012, 148 ff.

BGH, Urt. v. 25.10.2011, Az. VI ZR 93/10 = BGHZ 191, 219 ff.

BGH, Urt. v. 17.8.2011, Az. I ZR 57/09 – Stiftparfüm = BGHZ 191, S. 19 ff.

BGH, Urt. v. 17. 12. 2010, Az. V ZR 44/10 = BGH, NJW 2011, 753 ff.

BGH, Urt. v. 22.7.2010, Az. I ZR 139/08 - Kinderhochstühle im Internet I = GRUR 2011, 152 ff.

BGH, Urt. v. 30.6.2009, Az. VI ZR 210/08 = MMR 2009, 752 ff.

BGH, Urt. v. 26.06.2009, Az. VI ZR 196/08 – Spickmich = BGH, NJW 2009, 2888

BGH, Urt. v. 30.4.2008, Az. I ZR 73/05 – Internetversteigerung III = NJW-RR 2008, 1136 ff.

BGH, Urt. v. 19.4.2007, Az. I ZR 35/04 – Internetversteigerung II = BGHZ 172, 119 ff.

BGH, Urt. v. 27. 3. 2007, VI ZR 101/06 = NJW 2007, 2558

BGH, Urt. v. 20.7.2006 - I ZR 228/03 = NJW 2006, 3633 ff.

BGH, Urt. v. 11.3.2004, Az. I ZR 304/01 – Internet-Versteigerung I = BGHZ 158, 236 ff.

BGH, Urt. v. 17.5.2001, Az. I ZR 251/99 – ambiente.de = BGHZ 148, 13 f.

BGH, Urt. v. 11.12.1991, Az. VIII ZR 4/91 = BGHZ 116, 268 ff.

BGH, Urt. v. 19.9.1985, Az. III ZR 213/83 = BGHZ 95, 362 ff.

BVerwG, Beschl. v. 25.2.2016, Az. 1 C 28.14 = ZD 2016, 393 ff.

BVerwG, Urt. v. 6.9.1988, Az. 1 C 15.86 = DVBl. 1989, 59 f.

OVG Hamburg, Beschl. v. 29.6.2016 - 5 Bs 40/16 = ZD 2016, 450 ff.

OVG Schleswig, Urt. v. 4.9.2014 = ZD 2014, 643 ff.

OVG Schleswig, Beschl. v. 22.4.2013, Az. 4 MB 11/13 = ZD 2013, 364 ff.

OVG Koblenz, Urt. v. 26.1.2012, Az. 8 A 11081/11 = DVBl. 2012, 515 ff.

VG Hamburg, Beschluss v. 3.3.2016, Az. 15 E 4482/15 = ZD 2016, 243 ff.

VG Schleswig, Urt. v. 9.10.2013, Az. 8 A 14/12 = ZD 2014, 51 ff.

VG Schleswig, Beschluss v. 14.2.2013, Az. 8 B 60/12 = ZD 2013, 245 ff.

OLG Köln, Urt. v. 17.1.2014 Az. 6 U 167/13 = ZD 2014, 421 ff.

OLG Düsseldorf, Urt. v. 18.6.2013, Az. I-20 U 145/12, = K&R 2013, 594 ff.

OLG Hamburg, Urt. vom 27.6.2013, Az. 3 U 26/12 = ZD 2013, 511 ff.

OLG Dresden, Beschl. v. 8.2.2012, Az. 4 U 1850/11 = K&R 2012, 626 ff.

OLG Hamm, Beschl. v. 03.08.2011, Az. I-3 U 196/10 = CR 2012, 128 ff.

OLG Hamburg, Urt. v. 2.8.2011, Az. 7 U 134/10 = ZD 2011, 138 ff.

OLG Düsseldorf, Urt. v. 18.12.2007, Az. I-20 U 17/07 = MMR 2008, 682 ff.

OLG Frankfurt, Urt. v. 6.3.2007, Az. 6 U 115/06 = CR 2007, 454 f.

OLG Stuttgart, Urt. vom 22.2.2007 - 2 U 132/06 = MMR 2007, 437 f.

OLG Frankfurt, Urt. v. 30. 6. 2005 - 6 U 168/04 Skoda-Autokids-Club = GRUR 2005, 785 f.

OLG Düsseldorf, Urt. vom 20.02.2004 - 7 U 149/03 = ZUM-RD 2004, 236 f.

LG Düsseldorf, Urt. v. 9.3.2016, Az. 12 O 151/15 = ZD 2016, 231 ff.

LG Berlin, Urt. v. 28.10.2014, Az.16 O 60/13 = ZD 2015, 133 ff.

KG Berlin, Urt. v. 24.1.2014, Az. 5 U 42/12 = ZD 2014, 412 ff.

LG Potsdam, Urt. v. 31.7.2013, Az. 2 O 4/13 = MMR 2013, 662 f.

LG München I, Urt. v. 03.07.2013, Az. 25 O 23782/12 = CR 2013, 677 ff.

LG Berlin, Urt. v. 30.4.2013, Az. 15 O 92/12 = ZD 2013, 451 ff.

LG Regensburg, Urt. v. 31.01.2013, Az. 1 HK O 1884/12 = CR 2013, 197

LG Berlin, Urt. v. 6.3.2012, Az. 16 O 551/10 = ZD 2012, 276 ff.

LG Aschaffenburg, Urt. v. 19.8.2011, Az. 2 HK O 54/11 = MMR 2012, S. 38 ff.

KG Berlin, Urteil vom 25.09.2006 - Az. 10 U 262/05 = MMR 2007, 116 f.