Typoskript im Sinne des § 38 Abs. 4 UrhG. Das Original ist abgedruckt im Verwaltungsarchiv 107 (2016), S. 307-358.

Mario Martini*

Wie neugierig darf der Staat im Cyberspace sein?
Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen

I. Social Media Monitoring als Spürhund und Seismograph digitaler Kommunikationsbeziehungen

Im Mai 2014 – unmittelbar im Nachhall der NSA-Affäre – hat der BND die Republik mit einer sensiblen Ankündigung aufgeschreckt: Er will soziale Netzwerke in Echtzeit auswerten.[1] Mit dieser Idee ist der Auslandsgeheimdienst nicht allein. Auch das Verteidigungsministerium offenbarte wenig später, Meinungs- und Stimmungslagen der Bevölkerung schon seit geraumer Zeit mithilfe sozialer Netzwerke zu analysieren und die Ergebnisse künftig auch als Instrument der militärischen Gefahrenanalyse (etwa in Afghanistan) einsetzen zu wollen.[2] Das BKA, die Bundespolizei und der Zollfahndungsdienst nutzen schon länger offen zugängliche Informationen bei Facebook, Twitter und Co. zu Ermittlungszwecken.[3] Das BKA setzt seit dem Jahr 2000 die IBM-Software „Analyst's Notebook" ein: [4] Sie entwirrt das Beziehungsgeflecht zwischen Personen und hilft bei der Verifizierung bzw. Falsifizierung ermittlungsrelevanter Hypothesen. [5] Beim Kampf gegen extremistische Gewalt im Inneren führen der Verfassungsschutz und die Polizei als Teil des „Gemeinsamen Abwehrzentrums gegen Rechtsextremismus" (GAR) ein themenspezifisches

---

* *Mario Martini* ist Inhaber eines Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer und Leiter des Programmbereichs „Digitalisierung" am Deutschen Forschungsinstitut für Öffentliche Verwaltung Speyer. Der Autor dankt den Mitarbeitern im Programmbereich, allen voran Herrn *Michael Kolain*, *David Wagner*, *Quirin Weinzierl* und *Michael Wenzel*. Der Beitrag geht auf das deutsch-japanische Symposium „Die Verwaltung in der Gesellschaft der Netzwerke" vom 26./27.2.2015 zurück;. Der Autor widmet den Aufsatz seinem Doktorvater *Hans-Werner Laubinger* in Dankbarkeit zum 80. Geburtstag.

[1] Vgl. *Anonymous*, BND will soziale Netzwerke in Echtzeit ausforschen, Zeit Online vom 30.5.2014.

[2] *Reißmann*, Überwachung der Deutschen: So will die Regierung Facebook ausforschen, Spiegel Online vom 25.7.2014; *Fuchs*, Bundeswehr will soziale Netzwerke überwachen, Zeit Online vom 2.6.2014.

[3] Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE, BT-Drucks. 17/6587, S. 2. Vgl. zur polizeilichen Recherche in sozialen Netzwerken z. B. *Henrichs/Wilhelm*, Kriminalistik 2010, 30 (31 ff.); *Meyer*, Kriminalistik 2012, 759 (760 ff.); *Weichert*, Facebook, der Datenschutz und die öffentliche Sicherheit, in: Möllers/Ooyen (Hrsg.), Jahrbuch für öffentliche Sicherheit 2012/13, 2012, S. 379 (379).

[4] Antwort der Bundesregierung auf eine Kleine Anfrage der Fraktion DIE LINKE, BT-Drucks. 17/11582, S. 6. Vgl. zum verstärkten Einsatz von Big Data auf unionaler Ebene im Bereich von Europol insbesondere ErwGrd 7 u. 24, Art. 4 Abs. 1 lit. f, Abs. 2 und 3, Art. 18 Abs. 1-3, Art. 51 Abs. 3 lit. a der Verordnung 2016/794/EU des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für die Zusammenarbeit und die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (Europol) und zur Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates vom 11.5.2016, ABl. EU L 135, S. 53 ff.

[5] IBM hat auch eine Software mit dem Namen „i2 EIA" entwickelt (das Akronym steht für „Enterprise Insights Analytics"), die den Anspruch erhebt, aus Datensätzen (wie z. B. Reisepasslisten) Personen herauszufiltern, die mit Terroraktivitäten in Verbindung stehen. *Lobe*, Ist das ein Flüchtling oder ein Terrorist?, FAZ vom 17.2.2016, S. 13.

Internetmonitoring durch:[6] Seit Dezember 2011 durchkämmt die „Koordinierte Internetauswertung Rechtsextremismus“ (KIAR) den digitalen Kosmos, um dort Aktivitäten der rechten Szene zu beobachten. Sie hält beispielsweise Ausschau nach Hetze gegen Ausländer oder Hinweisen auf Angriffe gegen Flüchtlingsunterkünfte, wertet die Erkenntnisse umfänglich aus und leitet ggf. strafrechtliche Ermittlungen ein.

Doch nicht nur die Hüter der inneren und äußeren Sicherheit beobachten das Interaktionsgeschehen im Web 2.0:[7] Immer mehr Behörden und Unternehmen, aber auch die Kommunen[8] greifen für ihre Außenkommunikation auf soziale Netzwerke zurück, die – wie etwa bei einer Facebook-Fanpage[9] – als Abfallprodukt ihrer kommunikativen Funktion die Möglichkeit der strategischen Auswertung des Besucherverkehrs eröffnen. Zahlreiche Auswertungsprogramme

---

[6] Siehe *Bundesministerium des Innern*, Erstes Führungskräftekolleg Polizei und Verfassungsschutz, http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2012/06/fuehrungskraeftekolleg-polizei-verfassungsschutz.html (19.11.2015).

[7] Für das BKA ergeben sich besondere Befugnisse aus § 7 Abs. 2 BKAG zur Wahrnehmung der Aufgaben als Zentralstelle, ferner aus §§ 161 und 163 StPO beim Tätigwerden als Ermittlungsbehörde im Strafverfahren und aus § 20b BKAG für den internationalen Terrorismus; dazu auch bereits bspw. *Biemann*, „Streifenfahrten" im Internet, 2013, S. 162 ff. Diese Normen ermächtigen auch zum Handeln unter einer Legende: Bei der Teilhabe an der Kommunikation einer geschlossenen Benutzergruppe in einem sozialen Netzwerk können Ermittlungsmaßnahmen nach §§ 110a ff. StPO bzw. §§ 20l, 20g Abs. 2 Nr. 5, § 20m Abs. 2 BKAG zulässig sein (§§ 20l und 20g Abs. 2 BKAG verstoßen freilich gegen das GG und gelten nur übergangsweise fort, BVerfG, Urteil vom 20.4.2016, NJW 2016, 1781 [1796, Rdnr. 227 ff. zu § 20l (insbes. Art. 10 GG) und 1792, Rdnr. 175 ff. zu § 20g (Kernbereichsschutz)]). Für die längerfristige, gezielte Teilnahme an der Kommunikation in sozialen Netzwerken auf der Grundlage einer Legende setzt das BKA auf der Grundlage der §§ 110a ff. StPO sog. Virtuelle Verdeckte Ermittler ein; dazu etwa *Kudlich*, GA 2011, 193 (199); *Roggan*, NJW 2015, 1995 (1996). Vollständig neu sind diese technischen Möglichkeiten nicht. Sie komplettieren vielmehr das vorhandene Instrumentarium etwa der Rasterfahndung; vgl. §§ 98a und 98b StPO für den repressiven Einsatz bzw. die Polizeigesetze der Länder – etwa § 31 PolG NRW – und § 20j BKAG (dieser verstößt mit Blick auf die Löschungsfristen aus § 20j Abs. 3 Satz 3 BKAG jedoch gegen das GG und gilt nur übergangsweise fort, BVerfG, Urteil vom 20.4.2016, NJW 2016, 1781 [1794, Rdnr. 206 ff., 1800, Rdnr. 273). Eine Form der Internetaufklärung gestattet auch § 98c StPO: Personenbezogene Daten aus einem Strafverfahren dürfen mit anderen zur Strafverfolgung, Strafvollstreckung oder Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden, ohne dass dies in einer Errichtungsanordnung nochmals explizit Erwähnung finden muss. § 490 Satz 2 StPO entbindet von dem Erfordernis einer Errichtungsanordnung für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.
Auch die Anti-Terror-Datei hat einen im Online-Verbund nutzbaren Datenbestand geschaffen, der die Erkenntnisse von Polizei und Nachrichtendiensten im Bereich der Terrorismusbekämpfung zusammenführt, *Schaar*, RDV 2013, 223 (223). Das BVerfG hat ihrem Gebrauch mit Verweis auf den Grundgedanken des informationellen Trennungsprinzips jedoch Schranken aufgezeigt (BVerfG, Urteil vom 24.4.2013, BVerfGE 133, 277 [329, Rdnr. 123]).

[8] Nach einer Studie von *Drüke/Krellmann/Scholz et al.*, Wie nutzen Kommunen Social Media?, 2016, S. 12 f. nutzen 64 % der befragten Kommunen Social Media Angebote, weitere 7 % wollen diesen Kanal für sich noch im Jahre 2016 öffnen. 2013 nutzen nur 54 % Social Media. Zur Nutzung von Social Media Monitoring wiederum aber Fn. 33.

[9] Zu den mit der Einrichtung einer Facebook-Fanpage verbundenen datenschutzrechtlichen Fragen bspw. *Caspar*, ZD 2015, 12 (13 ff.); *Martini/Fritzsche*, NVwZ-Extra 21/2015, 1 ff. Vgl. auch den Beschluss des BVerwG vom 25.2.2016, ZD 2016, 199: Es hat den Rechtsstreit zwischen dem Unabhängigen Landeszentrum für Datenschutz (ULD) und der Wirtschaftsakademie Schleswig-Holstein dem EuGH vorgelegt.

ebnen inzwischen einen bequemen Weg, im Web 2.0 die Stimmung in der Bevölkerung zu beobachten und bei Bedarf gezielt abfragen.

All die Beispiele machen deutlich: Social Media Monitoring, also die systematische, sei es auf einzelne Personen,[10] sei es auf Menschengruppen auf der Grundlage anonymisierter Massendaten bezogene[11] Beobachtung, Filterung und Auswertung nutzergenerierter Inhalte sozialer Medien[12], entpuppt sich als eine für die informatorische, präventive und repressive Arbeit von Behörden attraktiven Form, das Datenlabyrinth sozialer Netzwerke zu erkunden und den dort versteckten Informationsschatz zu heben. Social Media Monitoring ist Teil eines nachhaltigen Strukturwandels, den Big Data-Technologien und semantische Analysewerkzeuge über die gesellschaftliche Ordnung und ihre Mechanismen der Entscheidungsfindung hereinbrechen lassen. Kaum haben die sozialen Netzwerke die Funktion von Flugblättern, Infoständen und Litfaßsäulen in ihrer viralen Verbreitungswirkung partiell abgelöst, sind sie auch in der Wahrnehmung von Behörden zusehends zu einer Fundgrube flächendeckender Datenauswertung avanciert. Im Web 2.0 spielt sich das „pralle Leben" einer digitalen Gesellschaft ab – vom Dating via Tinder und der frohen Kunde von der Geburt eines Kindes, über die Bekundung der politischen Meinung und hitzige Debatten bis hin zu persönlichen Bedrohungen und Cyber-Mobbing. Dank seiner Multifunktionalität und effizienten Algorithmensteuerung verheißt Social Media Monitoring, die Ernte stetig wachsender Datenfelder einzufahren und automatisiert die Spreu vom Weizen zu trennen.

Wie neugierig darf der Staat aber sein? So sehr Neugierde die Mutter des Fortschritts ist, so sehr ist sie auch der natürliche Feind der individuellen Freiheit; ihr Preis ist im schlimmsten Fall der Verlust der Privatsphäre als Keimzelle der persönlichen Entfaltung des mündigen Bürgers und die Erosion des Nährbodens einer pluralistischen und demokratischen Gesellschaft. Die Grenze zu erkennen, ab der der Staat auf den digitalen, in sozialen Netzwerken nur wenige Mausklicks entfernt liegenden Datenschatz als Instrument behördlicher Entscheidungsunterstützung zugreifen darf, ohne zu einem Überwachungsstaat zu mutieren, verlangt dem Gesetzgeber besonderes Feingespür ab.

Ungeachtet der Brisanz und Relevanz des Einsatzes von Social Media Monitoring-Technologien als Instrument der Entscheidungsunterstützung durch öffentliche Stellen schweigt sich die juristische Literatur zu seiner Zulässigkeit bislang aus.[13] Der Beitrag stellt sich der Herausforderung, das Potenzial und die Funktionsweise (1.-4.) sowie den verfassungsrechtlichen (II.) und einfachgesetzlichen (III.) Rahmen für das Social Media Monitoring öffentlicher Stellen auszuloten.

---

[10] Dazu unten I. 5. b. bb., S. 15.

[11] Dazu unten I. 5. b. aa., S. 13.

[12] Der Aufsatz legt der Wendung „Social Media Monitoring" ein weites Begriffsverständnis zugrunde. Vgl. zum Begriff auch *Aßmann/Pleil*, Social Media Monitoring: Grundlagen und Zielsetzungen, in: Zerfaß/Piwinger (Hrsg.), Handbuch Unternehmenskommunikation, 2007, S. 585 (587); *Schulz/Hoffmann*, Soziale Medien in der öffentlichen Verwaltung, PdK - Band L 16 Bund, 2013, Rdnr. 66.

[13] Es finden sich zwar Beiträge zum Social Media Monitoring der Unternehmenswelt [vgl. z. B. *Aßmann/Pleil* (Fn. 11); *Schreiber*, PinG 2 (2014), 34 ff.; *Venzke-Caprese*, DuD 2013, 775 ff.], aber nicht ein einziger zu dem ungleich sensibleren Monitoring öffentlicher Stellen.

Die Analyse macht deutlich, dass dem Monitoring gegenwärtig die Tür recht weit offensteht und im digitalen Zeitalter normative Anpassungen geboten sind (IV.-V.).

1. Auswertungspotenziale sozialer Netzwerke

„Die Kraft, große Dinge zu entscheiden, kommt aus der ununterbrochenen Beobachtung der kleinen Dinge." Mit dieser Weisheit skizzierte *Gerd Bucerius* – weit vor Anbruch der digitalen Revolution – geradezu die Blaupause für modernes Social Media Monitoring: Dessen Wesen besteht darin, aus dem Echolot sozialer Netzwerke Signale für das eigene Handeln abzuleiten und daran den eigenen Handlungskompass auszurichten. Dabei macht es sich die besondere Eigenschaft sozialer Netzwerke zunutze: Sie sind Megafone der Selbstdarstellung und Sensoren sozialer Kommunikations- und Interaktionswellen. Sie zeichnen das persönliche Beziehungsgeflecht der Menschen und die viralen Effekte ihrer Kommunikation in einer bisher nicht da gewesenen Präzision nach – und projizieren dadurch ein detailgetreues Ebenbild der sozialen Realität an die digitale Analyseleinwand.[14] In dem Maße, in dem soziale Netzwerke die Kommunikationsmöglichkeiten der Nutzer erweitern, setzen sie deren digitales Verhalten zugleich einer konstanten Beobachtung aus. Nicht nur der unerschöpflich große Datenschatz aus persönlichen Informationen und Vorlieben (z. B. Lieblingsfilmen, Freizeitinteressen und Konsumpräferenzen), den ein breiter Querschnitt der Bevölkerung aus freien Stücken im Web 2.0 als digitalen Fußabdruck hinterlässt, ist es, der einen Zugang zum Datenpool von Facebook, Twitter und Co. so reizvoll macht. Auch die (jedenfalls subjektiv wahrgenommene) Vertrauenswürdigkeit der Informationen für die Zielgruppe sowie die ubiquitäre Verfügbarkeit, Persistenz, Strukturierung und Durchsuchbarkeit der Informationsgehalte verleihen ihm ein Alleinstellungsmerkmal.[15] So schnell, wie die Beiträge entstehen und sich verbreiten, so rasch und kostengünstig lassen sie sich mit der Hilfe von Big Data-Algorithmen sowohl für öffentliche als auch für kommerzielle Zwecke auswerten. Der Schatz personenbezogener Informationen, der in sozialen Netzwerken schlummert, ist größer als all das, was das Ministerium für Staatssicherheit der DDR mit seinem großflächigen Apparat über die Bevölkerung jemals hätte sammeln können.

2. Gegenstand eines Social Media Monitorings

Social Media Monitoring greift vorrangig auf die im Web 2.0 geteilten Inhalte und geäußerten Präferenzen („Likes") der Nutzer zu. Hinzu kommen Gruppenmerkmale wie Alter, Geschlecht, Wohnort, Qualifikation oder Arbeitgeber. Die so gewonnenen Informationen gehen über den

---

[14] Verzerrt werden kann dieses Spiegelbild allerdings durch die Steuerung, welche die Algorithmen des Netzwerks bei der Nachrichtenverteilung übernehmen und damit – ähnlich wie eine Nachrichtenredaktion – einen Filter über die soziale Kommunikation legen. Vgl. dazu und zur Notwendigkeit einer Algorithmenkontrolle *Martini*, Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz, in: Hill/Martini/Wagner (Hrsg.), Die digitale Lebenswelt gestalten, 2015, S. 97 (151).

[15] *Hofmann*, Methoden des Social Media Monitoring, in: König/Stahl/Wiegand (Hrsg.), Soziale Medien, 2014, S. 161 (161); vgl. auch *Oermann/Staben*, Der Staat 52 (2013), 630 (652); *Schmid*, Das neue Netz, 2. Aufl., 2011, S. 119 f.

Erkenntniswert hinaus, dass Videos von Babykatzen in der Netzcommunity besonderen Anklang finden. Sie können beispielsweise in das Ergebnis münden: Junge Erwachsene im Alter zwischen 20 und 30 Jahren diskutieren zunehmend kontrovers (und ggf. sogar radikal) über ein Infrastrukturprojekt, das kurz vor Baubeginn steht. Oder: Im Raum „Musterstadt“ häufen sich Social Media-Posts, die Hinweise auf fremdenfeindliches, in einzelnen Fällen strafrechtlich relevantes Verhalten enthalten. Aber auch statistische Nutzerdaten, etwa Verweildauern auf Websites, sind Gegenstand der Beobachtung. Sie geben Aufschluss über die quantitative Nutzung bestimmter Inhalte und das individuelle Surfverhalten sowie darüber, wie sich im Cyberspace mediale Aufmerksamkeit erzeugen lässt und welche Ausgestaltung der Inhalte zum längeren Verweilen und welche tendenziell zum Weiterklicken einlädt.

Anders als sein „kleiner Bruder“ Social Media Analytics zielt Social Media Monitoring weniger auf die punktuelle Auswertung einzelner Social Media-Präsenzen zu einem bestimmten Zeitpunkt (z. B. die Reichweite eines Beitrags auf der Facebook-Seite der Stadt Freiburg am Karfreitag zum Thema „Tanzverbot“), sondern auf die fortwährende Beobachtung langfristiger Entwicklungen im Zeitstrahl – jeweils nicht nur zu dem Verhalten von Gruppen oder der Gesamtbevölkerung, sondern durchaus auch von Einzelpersonen. Aufgabe des Monitorings ist es dann, aus den im digitalen Raum gesammelten Erkenntnissen maßgeschneiderte Handlungsempfehlungen abzuleiten. Die Ergebnisse können als Frühwarnsystem für sich ausbreitende Fehlentwicklungen dienen, denen sich dann durch die richtige Kommunikationsstrategie rechtzeitig begegnen lässt. Im besten Fall machen sie umfangreiche Trendstudien oder aufwändige Meinungsumfragen weithin überflüssig. Gerade sein Potenzial zur Ressourceneinsparung und die nutzerfreundliche Ausgestaltung der (teils kostenlosen) Software machen auch für die Verwaltung den besonderen Charme des Social Media Monitorings aus – ebenso aber seine machtvolle Eignung, die Nadel im kaum übersehbaren Heuhaufen der Daten dort zu finden, wo Einzelne – bewusst oder unbewusst – Gesetzesverletzungen auf der Agora des Cyberspace begehen oder dokumentieren.

3. Datenquellen

Die Datenquellen des Social Media Monitorings erschöpfen sich nicht allein in Profilen sozialer Netzwerke, die vorrangig dem unmittelbaren Informationsaustausch der Nutzer dienen, wie Facebook, Google+ oder XING. Sie erstrecken sich auch auf nutzergenerierte Plattformen, die dem Wissensaustausch verschrieben sind, insbesondere Wikis [16] , Blogs [17] , Internetforen und

[16] Darunter versteht man hypertext-basierte Webseiten, deren Inhalte Benutzer online ändern und ergänzen können.
[17] Der Begriff steht für auf einer Webseite geführte Logbücher, die Inhalte protokollieren.

Bewertungsplattformen sowie auf Social Bookmarking[18]. Hinzu kommen Portale, die auf das Teilen und Kommentieren von (insbesondere audiovisuellen) Inhalten angelegt sind, wie z. B. YouTube, Flickr und Instagram.[19] Die Datenquellen lassen sich damit drei (nicht schnittmengenfreien) Nutzungsklassen zuordnen: soziale Kommunikation, Wissensaustausch und Teilen von Inhalten.

4. Funktionsweise

Die anwachsenden Datenwälder des Internets durchforsten Social Media Monitoring-Tools systematisch, um mit ihrer Hilfe komplexe Interaktions- ebenso wie individuelle Handlungsmuster ausfindig zu machen und die daraus gewinnbaren Erkenntnisse nutzergerecht aufzubereiten. Das Web 2.0 legt das individuelle und kollektive Stimmungsbild der Netzgemeinde in seiner Vielschichtigkeit frei. Moderne Sentimentanalysen beherrschen inzwischen mit erstaunlicher Detailgenauigkeit die Kunst, die Tonlage der Stimmungen und Schwingungen aus Textbeiträgen zu enträtseln und daraus greifbare Aussagen zu generieren.

Auf die Inhalte der sozialen Netzwerke lässt sich entweder durch plattformeigene Analyseinstrumente (z. B. Facebook Insights) oder über Auswertungsprogramme von Drittanbietern (etwa Google Analytics)[20] zugreifen, die den Zugang zum Netzwerk über eine Schnittstelle des Diensteanbieters (sog. Application Programming Interfaces – APIs) eröffnen. So tummeln sich Social Media Monitoring-Programme inzwischen in reicher Zahl auf dem Markt – beginnend von Talkwalker, Brandwatch, Echobot, über Sysomos, Vico Analytics und uberMetrics bis hin zur kostenlosen Social Media-Suchmaschine socialmention.com. Auch der Bund hält mit Xpider einen eigenen sog. Webcrawler[21] vor: Er durchsucht insbesondere Verkaufsplattformen auf mögliche Verdachtsfälle für Steuervergehen.[22]

Alle Analyseformen des Social Media Monitorings haben regelmäßig einen gemeinsamen Ausgangspunkt: die *Indizierung von Schlüsselbegriffen*, auf deren Auswertung (insbesondere hinsichtlich Häufigkeit, Verwendungskontext und Tonalität) sich die Beobachtung als Dreh- und

---

[18] Der Begriff beschreibt Lesezeichen, die mehrere Nutzer im Internet zum Zweck wechselseitiger Information austauschen.

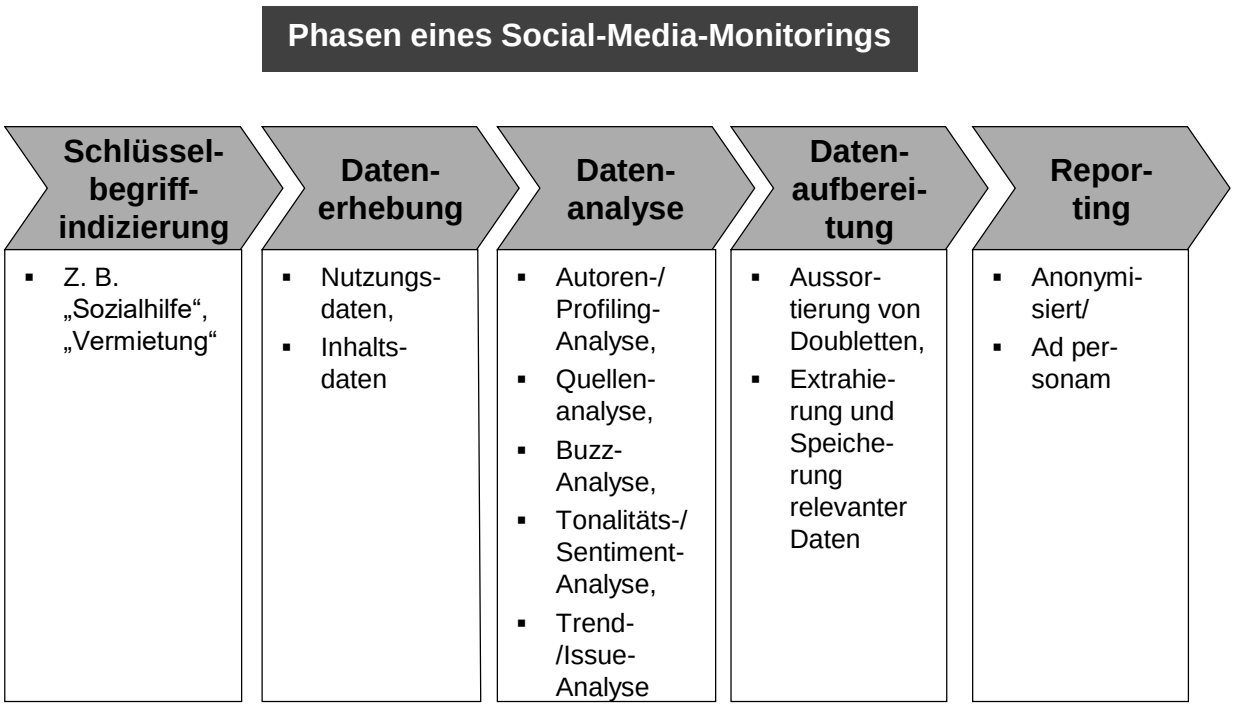
[19] Zu den Datenquellen des Monitorings siehe allgemein *Sen*, Social Media Monitoring für Unternehmen, 2011, S. 77 ff.

[20] Bei Google Analytics handelt es sich um ein Programm, das seinen Kunden statistische, anonymisierte Informationen über die Nutzung der eigenen Internetseite und die Struktur der Nutzergruppe (z. B. Geschlecht, Herkunft der Besucher und ihre Verweildauer) zur Verfügung stellt, um den Internetauftritt an die Bedürfnisse der Interessenten anpassen zu können, *Schulz/Hoffmann* (Fn. 11), Rdnr. 69 f. i. V. mit 66.

[21] Der Begriff bezeichnet im Englischen (to crawl) bildhaft das Durchstöbern bzw. Durchkriechen einer Webseite. Darin kommt treffend zum Ausdruck, dass das Instrument jeweils auf die umfassende Auswertung der Inhalte und Interaktionsmuster zielt.

[22] *Bundeszentralamt für Steuern*, Xpider, http://www.bzst.de/DE/Steuern_International/USt_Betrugsbekaempfung/Internet_Ermittlung/Internet_Ermittlung.html?nn=23442 (25.4.2016).

Angelpunkt richtet. Daran schließen sich typischerweise vier weitere Phasen an:[23] Am Anfang steht die *Datenerhebung* mittels eines Webcrawlers, also die Beschaffung von Informationen durch Auffinden und Speichern aller Beiträge, die den Schlüsselbegriff enthalten. In der Phase der *Datenaufbereitung* sortieren Programme Spam und Doubletten aus und extrahieren sowie speichern Metadaten – also die Social Media-Inhalte beschreibende Daten, etwa Erstelldatum, Verweildauer auf der Website oder Schlagwörter eines Beitrags. Das Herzstück des Monitorings bildet die *Datenanalyse*: Sie generiert aus den aufbereiteten Daten Wissen. In sehr unterschiedlicher Form lässt sie sich konzipieren. Beliebt sind insbesondere *Autoren- und Profiling-Analysen*, um Meinungsführer zu identifizieren, [24] die als Knotenpunkte im sozialen Netz maßgeblichen Einfluss auf die Verbreitung von Informationen haben, und Profile von ihnen anzulegen. Eine *Relevanz- und Quellenanalyse* hingegen durchsucht das Netz nach speziellen Themen, ihrer Reichweite und ihrem Einflusspotenzial.[25] Zum Einsatz kommen auch *Buzz-Analysen*, die Informationen über die Einbindung einer Zielgruppe in ein spezielles Thema[26] generieren. Mit der Verfeinerung der technischen Möglichkeiten erlangen *Tonalitäts- bzw. Sentimentanalysen*, also die Ermittlung des Meinungsbilds der Zielgruppe und der Stimmungslage, sowie *Trend- und Issue-Analysen,* welche die Entwicklung von Themen für Social Media-Auftritte kontinuierlich evaluieren, wachsende Bedeutung. Die Datenanalyse mündet regelmäßig in eine *Reporting-Oberfläche*, welche die gesammelten Informationen als Instrument der Entscheidungsunterstützung (häufig visuell in sog. Dashboards) aufbereitet und in einer Datenbank aggregiert, die sich auf Schlüsselwörter durchsuchen lässt.[27] Das Monitoring kann aber auch mit einer Identifizierung einzelner Personen enden, die zur Zielscheibe behördlicher (oder unternehmerischer) Maßnahmen werden.



5. Anwendungsfelder und Chancen

a) Kommerzielle Nutzung durch Private

Den Trend zum Social Media Monitoring haben Unternehmen gesetzt. Für viele Firmen ist das wertschöpfungsorientierte Durchforsten sozialer Netzwerke längst ein Grundpfeiler ihrer Unternehmensstrategie. Sie nutzen deren Kommunikationspotenzial zur Marktforschung und setzen es als strategischen Rückkanal der Unternehmenskommunikation ein, um die Strahlkraft und Wirkmacht ihrer Marke durch ein virales Marketing zu stärken.

Im analogen Zeitalter prägte noch die defätistische Grundhaltung *Henry Fords* die Entscheidung über das unternehmerische Werbebudget: „Die Hälfte meiner Werbeausgaben ist zum Fenster hinausgeworfen. Ich weiß nur nicht welche Hälfte." Die Werbenden streuten möglichst breit und hofften, die Zielgruppe durch Plakate, Flyer und Marketing-Aktionen zu treffen. Social Media Monitoring verheißt nun, die rentable Hälfte der Werbeausgaben zu identifizieren und damit eine höhere Trefferquote zu erzielen. Die Tage teurer, mit langer Vorlaufzeit und Streuverlusten verbundener Printprodukte scheinen gezählt. Die Onlinesparte ist zum unbestrittenen Flaggschiff moderner Werbeagenturen avanciert.
Im digitalen Zeitalter verschiebt sich auch die innere Logik erfolgreicher Markenwerbung. Während bislang die Unternehmen die Kundenansprache und die Entwicklung ihrer Reputation durch eigenes Handeln dominierten, dreht sich die Entwicklung nun um: Die Kommunikationskanäle im Internet entfalten eine Eigendynamik. Kunden tauschen sich im World Wide Web über Produkte und Marken aus – ob die Unternehmen das wollen oder nicht. Beeinflussen können Firmen nur, ob sie an der Kommunikation teilhaben oder ob diese ohne sie stattfindet.

Aus einem Blog oder Bewertungsportal heraus kann schnell ein für das Unternehmen gefährliches Reputationsrisiko erwachsen. Schmerzhaft bekam das etwa das Unternehmen O2 im Falle der „Wir sind Einzelfall"-Initiative eines in Warteschleifen vertrösteten Kunden zu spüren: Der Sturm, den sie

entfachte, ließ Wellen des Spotts über den Telekommunikationsriesen hereinbrechen.[28] Dem Konzern entstand dadurch ein beträchtlicher Ansehensverlust. Umgekehrt können Flüsterkampagnen sozialer Netzwerke – ob spontan oder durch gezielte Marketingstrategie – geradezu einen Boom der Bekanntheit auslösen und aus einem Zwerg einen Riesen machen, wie etwa die explosionsartig gestiegenen Klickraten eines Videos der Poetry-Slammerin *Julia Engelmann* zeigen.

Unter dem Leitmotiv „wissen, was passiert" richtet Social Media Monitoring sein Sensorium auf potenziellen Kunden aus, um eine Gemeinschaft mit den Zielgruppen aufzubauen. Denn die Unternehmen wissen: Ihre digital vernetzten Kunden sind die besten Werbeträger. Das soziale Netz verleiht Formen mittelbarer Werbung neues Macht- und Wirkungspotenzial. Firmen erreichen dort die Gefühlslagen der Kunden zielgenauer und nachhaltiger. Je besser sie die Bedürfnisse ihrer Zielgruppen sowie Märkte und Trends ergründen, umso schneller können sie auf diese reagieren und ggf. aufbrausende Empörungswellen frühzeitig brechen. Nur wer den Anregungen und Ideen der Nutzer einen hohen Stellenwert beimisst, kann ihnen wertvolle Impulse für die Weiterentwicklung eigener Produkte und Dienstleistungen entnehmen. Social Media Monitoring legt daher das Ohr an das Herz des Internetnutzers, um den Schwingungen seiner Emotionen und Bedürfnisse nachzuspüren. Eben dies ist das Geheimnis guter Werbung: Sie besteht (cum grano salis) in der Kunst, auf das Herz zu zielen und die Brieftasche zu treffen.[29] Der Umgang mit den Möglichkeiten und Chancen des Web 2.0 ist letztlich Ausdruck der kommunikativen, kurativen Grundhaltung eines Unternehmens. Dass die Unternehmen dies verstanden haben, spiegelt sich auch in Zahlen wider: Bereits die Hälfte aller Unternehmen mit mehr als 500 Mitarbeitern macht sich die Vorteile des Social Media Monitorings zunutze.[30] Die meisten (70 %) setzen es als Marketinginstrument mit dem Ziel ein, die Wirkung ihrer Produkte, Dienstleistungen und Werbestrategien auf dem relevanten Markt zu analysieren; nur knapp die Hälfte verwendet es zu weiteren Zwecken, etwa zur externen Kommunikation oder für den Kundenservice.[31] Sie folgen damit dem digitalen Imperativ, den *Bill Gates* treffend in die Worte kleidete: „Das Internet ist wie eine Welle: Entweder man lernt, auf ihr zu schwimmen, oder man geht unter."
Mittelständische Unternehmen springen auf das „Surfbrett" Social Media Monitoring hingegen noch zurückhaltend auf; nur 10 % nutzen es.[32] Dabei kann gerade für kleine und mittlere Firmen, denen nur begrenzte Ressourcen für die Marktforschung und Kundenanalysen zur Verfügung stehen, die Nutzung und Auswertung digitaler Marketingkanäle sozialer Medien besonders wertvoll

---

[28] *Spehr*, Hat O2 ein Problem?, FAZ.net vom 21.11.2011.
[29] Angelehnt an einen Aphorismus von *Vance Packard.*
[30] Vgl. *BITKOM*, Leitfaden Social Media, 2. Aufl., 2012, S. 16; vgl. auch *Erster Arbeitskreis Socialmedia B2B*, B2B und Social Media – Wie verändert sich die Nutzung der Kanäle?, 2016, S. 6 mit einem (angesichts des Studiendesigns nicht repräsentativen) Ländervergleich zwischen Deutschland und Österreich.
[31] Vgl. *BITKOM* (Fn. 29), S. 16.
[32] *BITKOM* (Fn. 29), S. 5, 7 und 40.

sein: Detailgenaue Kenntnisse über (potenzielle) Kunden ebnen ihnen einen kostengünstigen Weg, diese zielgenau zu adressieren und bedarfsgerecht zu informieren. Nicht umsonst ist die Online-Reputation zu einem Kernelement des Markenbildes eines Unternehmens avanciert. Für viele Start-ups mit junger Zielgruppe sind soziale Netzwerke oftmals ihr einziges Schaufenster und ausschließlicher Kommunikationskanal zu ihrer Community; die effiziente Analyse des digitalen Grundrauschens ist für sie daher häufig überlebenswichtig – Pressemitteilungen, Newsletter oder ein Büro mit Festnetzanschluss gehören für sie weitgehend der Vergangenheit an, bieten doch soziale Medien die notwendige Infrastruktur gebündelt und aus einer Hand an.

Ob in großen oder kleinen Unternehmen: Von klassischen Kommunikationsstrategien heben sich Maßnahmen eines Social Media Monitorings durch einen nur schwer einholbaren Vorzug ab. Anders als in der analogen Welt lassen sich die Effekte unternehmerischer Marketingmaßnahmen, z. B. Werbekampagnen oder Produkteinführungen, schnell, günstig und vergleichsweise präzise messen. Eine kontinuierliche Analyse des Lichtes, in dem Dritte ein Unternehmen sehen (sog. Reputationsmessung), wird ebenso möglich wie eine Kampagnenevaluation und eine Erfolgskontrolle eigener Marketing- und Social Media-Maßnahmen. Auf dieser Grundlage lässt sich die strategische Zielsetzung später mit dem Erreichten abgleichen, um daraus die operativen Konsequenzen für das eigene Optimierungsmanagement zu ziehen.

b) Öffentliche Stellen

Auch öffentlichen Stellen steht der Nutzen von Social Media Monitoring immer klarer vor Augen. Aufschlussreich sind für sie nicht alleine die öffentliche Wahrnehmung der eigenen Behörde oder Kommune [33], die Evaluation ihrer Online-Angebote oder PR-Kampagnen und das Wissen um themenspezifische Stimmungsbilder in der Bevölkerung auf der Grundlage aggregierter Massendaten (aa).[34] Vielmehr steuert Social Media Monitoring in wachsendem Umfang auch die inhaltliche Arbeit der Behörden bis hin zur Unterstützung bei der Entscheidungsfindung in Einzelfallsituationen auf der Grundlage personenbezogener Beobachtungsmechanismen (bb).

---

[33] Kommunen nutzen in geringerem Umfang Social Media Monitoring. 51 % nutzen dieses Instrument nicht; entgegen dem Trend zur verstärkten Nutzung von Social Media auch auf kommunaler Ebene (vgl. Fn. 8) hat diese Zahl sogar zugenommen, 2013 waren es 43 %, *Drüke/Krellmann/Scholz et al.* (Fn. 8), S. 20 f. Professionelles automatisiertes Social Media Monitoring, wie es im Mittelpunkt dieses Beitrags steht, nutzt sogar nur eine befragte Kommune. Diese geringe Quote resultiert nach Ansicht der Studienautoren vor allem aus der Nutzung von Social Media auf kommunaler Ebene, die eher auf Informationsverbreitung als auf Interaktion ausgerichtet ist, a. a. O., S. 21.

[34] *Bundesministerium des Innern*, Leitfaden Krisenkommunikation, 2014, S. 23. Im Wahlkampf nutzen die Parteien (als nicht-öffentliche Stellen) soziale Netzwerke schon länger als Stimmungsbarometer, um die verschiedenen Multiplikatoren und ihre Themen zu identifizieren, aggregieren und analysieren. Dazu beispielsweise *Fischoeder/Kirsch/Visser et al.*, Social Media-Monitoring in der Praxis am Beispiel des Bundestagswahlkampfes 2009, in: Brauckmann (Hrsg.), Web-Monitoring, 2010, S. 349 (352 ff.).

aa) Social Media Monitoring auf der Grundlage aggregierter Massendaten

Social Media Monitoring, das auf der Grundlage aggregierter Massendaten erfolgt, konzentriert sein Erkenntnisinteresse auf die Analyse von Stimmungen, Trends und Entwicklungen. Das Persönlichkeitsinteresse Betroffener beeinträchtigt es nur eingeschränkt (nämlich bei der Datenerhebung).

(1) Politische Steuerung und Kommunikation der öffentlichen Verwaltung

Massendatenbasiertes Social Media Monitoring öffentlicher Stellen ist ein Sensorium der Gefahrenabwehr und ein Spürhund politischer Kommunikation. Es beobachtet sich verändernde Stimmungsströme und richtet den administrativen wie politischen Kompass auch an dieser Koordinate aus. Sein Einsatzspektrum reicht von der Krisenerkennung[35] durch ein automatisiertes Filter- und Bewertungssystem [36] über die Erschließung von Helferpotenzialen bei der Krisenbewältigung[37] und die Risikoprävention bei Großveranstaltungen, wie Sportereignissen, bis hin zur Begleitung und Analyse aktuell diskutierter Themen und Trends, die einen Bezug zum Verwaltungshandeln aufweisen.[38] Das schließt eine Präferenzanalyse und die Identifikation von Optimierungspotenzialen sub specie staatlicher Dienstleistungen sowie die Zufriedenheit mit dem demokratischen System ein – nicht zuletzt auch die Evaluation (neuer) gesetzlicher Regelungen und die Analyse eines Bedarfs nach staatlicher Intervention.[39] All diese Anwendungsfelder haben das Potenzial, die Arbeit der öffentlichen Verwaltung in Zeiten der Digitalisierung zu verändern.

(2) Bürgerpartizipation

Social Media Monitoring kann auch das Mitmachpotenzial der Bevölkerung erschließen und gesellschaftliche Wissensreservoirs heben. Es kann dazu beitragen, Defizite in der öffentlichen Kommunikation staatlicher Stellen sichtbar zu machen und im Idealfall zu überwinden. Mit den

---

[35] Dazu gehört die Analyse und Prognose der Verbreitung eines Grippevirus ebenso wie die Erdbebenerkennung oder die Vorhersage von Flüchtlingsströmen.

[36] *Zisgen/Kern/Voßschmidt*, Bevölkerungsschutz (3) 2014, 9 (11).Vgl. auch *Bundesministerium des Innern* (Fn. 32), insbesondere S. 14 und 24.

[37] Vgl. in diese Richtung *Lüge*, Bevölkerungsschutz (3) 2014, 4 (5). Die US-Behörde IARPA hat in den USA ein sog. OSI-Programm (OSI steht für „open source indicators“) aufgelegt. Es zielt darauf, öffentlich verfügbare Daten kontinuierlich zu analysieren, um auf dieser Grundlage politische, humanitäre oder soziale Krisen zu identifizieren, siehe http://www.iarpa.gov/index.php/research-programs/osi (17.4.2016). Zur Krisenintervention mittels Social Media Monitoring in den USA siehe auch *Grün*, Terroristenjagd im sozialen Netz, Zeit Online vom 13.8.2011. Im Zuge der Unruhen im August 2014 nutzte die Polizei den Social Media Monitoring-Dienst „Geofeedia“ um Demonstranten zu überwachen, *Anonymous*, Analysefirma nutzt Zugang zu sozialen Medien für US-Polizei aus, Spiegel Online vom 12.10.2016.

[38] *Fuchs*, Social-Media-Instrumente im Schatten von Facebook und Twitter Best Practice-Beispiele aus deutschen Verwaltungen, in: Hill (Hrsg.), E-Transformation, 2014, S. 175 (179).

[39] Vgl. etwa für die Bundesagentur für Arbeit Plenarprotokoll des Deutschen Bundestages 18/78 vom 14.1.2015, S. 7466.

Instrumenten seiner automatisierten Auswertung lässt sich nachvollziehen, an welcher Stelle der Argumentations- oder Erklärungskette bei den Bürgern eine Lücke entstanden ist. Missverständnisse lassen sich dann ausräumen, bevor sie sich im öffentlichen Diskurs verfestigen.

Das Monitoring und die Analyse digitaler Dialoge in sozialen Medien können helfen, Themen für Bürgerkonsultationen bedarfsgerecht zuzuschneiden und die richtigen Multiplikatoren (z. B. NGOs oder Bürgervereinigungen) sowie geeignete Partizipationswerkzeuge ausfindig zu machen.[40] Soweit das Social Media Monitoring Defizite bei der Aktivierung von Beteiligungspotenzialen offenlegt, können gezielte Informationskampagnen in den einschlägigen sozialen Medien das Beteiligungsinteresse steigern und den Beteiligungsertrag potenziell erhöhen.

Mit Hilfe von Monitoring-Tools lässt sich nicht nur abbilden, welche Gruppen sich von konkreten staatlichen Planungen und Entscheidungen besonders betroffen fühlen; sie lassen sich auch gezielter adressieren, ist doch eigene Betroffenheit die wichtigste Triebfeder für die Nutzung öffentlicher Partizipationsangebote: Wer erkennt, dass der eigene Wirkungskreis berührt ist, will regelmäßig Einfluss auf den Ausgang einer partizipativen Diskussion nehmen, seine Präferenzen mitteilen oder Lösungsansätze beisteuern. Sich anbahnende Empörungswellen lassen sich so rechtzeitig in geordnete Bahnen lenken, bevor sie die Straßen und das Web 2.0 mit sich radikalisierendem und inhaltlich nur noch schwer zugänglichem Protest füllen.

Eine Vorfeldanalyse bürgerlichen Beteiligungsbedarfs via Social Media Monitoring aktiviert staatliche Kommunikationssensoren, die als Frühwarnsysteme diejenigen Themen aufspüren, für die eine Online-Partizipation angezeigt ist (oder mit der umgekehrt lediglich eine Verschwendung von Haushaltsressourcen einhergeht). Social Media Monitoring ist insofern auch Teil einer proaktiven Staatskommunikation.[41] Beteiligungsanliegen artikulieren sich in sozialen Medien ungefilterter und offener. Sie lassen sich dadurch differenzierter aufschlüsseln, als das beispielsweise im Rahmen einer Bürgersprechstunde oder an einem Infostand auf dem Marktplatz möglich ist. Die softwaregestützte Auswertung einer Debatte zu einem bestimmten Beteiligungsverfahren ist in der Lage, den Funktionswert des Verfahrens (z. B. einer Bürgerbefragung) und seinen Informationsstrom – jedenfalls quantitativ – messbar zu machen sowie eine etwaige Selektivität der Beteiligung offenzulegen.[42] Die gewonnenen Erkenntnisse ermöglichen den staatlichen Entscheidungsträgern, Beteiligungsergebnisse rational zu würdigen,

[40] Wichtig ist das nicht zuletzt vor dem Hintergrund nach wie vor und insbesondere auch online bestehender partizipativer Gräben. Bislang bewegen sich Beteiligungsquoten in Partizipationsportalen regelmäßig im Promillebereich.
[41] Vgl. dazu *Hill*, JZ 1993, 330 ff.
[42] *Martini/Fritzsche*, Kompendium Online-Bürgerbeteiligung, 2015, S. 92.

sozio-demografische Ungleichgewichte der Beteiligung im Auge zu behalten und nicht-repräsentative Interessenbekundungen auszubalancieren.

bb) Monitoring ad personam

Ebenso wie eine vom Einzelnen abstrahierende Massendatenanalyse gehört ein Social Media Monitoring, das Nachforschungen über individuelle Personnen oder auf sie bezogene Daten in sozialen Medien anstellt, zum Handlungsrepertoire der öffentlichen Verwaltung. Es berührt den einzelnen Bürger am unmittelbarsten und in rechtlich sensibelster Weise.

(1) Nachforschungen der Melde-, Steuer- und Sozialbehörden

Dass die Melde- und Steuerbehörden die Profile sozialer Netzwerke ausforschen, um Zweitwohnsitze oder verschwiegene Zusatzeinnahmen, etwa beim Online-Marktplatz eBay oder der Wohnungsbörse Airbnb, auszumachen, ist längst keine Zukunftsvision mehr: § 5 Nr. 17 des Finanzverwaltungsgesetzes weist dem Bundeszentralamt für Steuern bei der Umsatzbesteuerung des elektronischen Handels ein solches Monitoring zur Unterstützung der Landesfinanzverwaltungen ausdrücklich als Aufgabe zu. In der Netzcommunity lässt die staatliche Inspektion der Datensilos von Facebook, Twitter und Co. bereits Fantasien zu möglichen weiteren Verwendungszwecken aufkeimen – etwa das Szenario einer Überprüfung der Netzprofile von Hartz IV-Empfängern auf verschwiegene Einnahmen. Dass die Bundesagentur für Arbeit im Jahre 2014 ein Tool ausgeschrieben hat, das Diskussionen und Kommentare im deutschsprachigen Social Web analysieren soll,[43] hat entsprechende Spekulationen zusätzlich befeuert.

Der Grat zwischen Social Intelligence und Surveillance, zwischen legitimer Informationsbeschaffung und unzulässiger Überwachung ist schmal. Welche dunkle Seite ein weitgreifendes Social Media Monitoring des Staates haben kann, macht eine Ankündigung der chinesischen Regierung deutlich: Sie hat für das Jahr 2017 ein Sozialpunktesystem angekündigt, das große Datenmengen über jede Organisation und jeden Bürger, etwa über soziales Verhalten und die Navigation im Netz, sammelt und Regierungsstellen zur Verfügung stellt.[44] Die Datenbank sollte ursprünglich Steuerbetrug sowie Verletzungen von Urheberrechten verhindern. Nunmehr soll das System in den Dienst der Sicherung „sozialistischer Werte“ treten. Eine Vollerhebung der digitalen Kommunikation soll gesellschaftliche

---

[43] Die Leistungsschreibung der mittlerweile beendeten Ausschreibung findet sich unter http://www.monitoringmatcher.de/wp-content/uploads/2015/08/monitoringmatcher_bundesagentur_leistungsbeschreibung.pdf (27.4.2016).

[44] *China Copyright and Media*, Planning Outline for the Construction of a Social Credit System (2014-2020), https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (19.4.2016); *Kolonko*, Punkte für Wohlverhalten, FAZ vom 7.5.2015, S. 5.

Spannungen reduzieren und die Bürger zur Ehrlichkeit erziehen. Damit nimmt eine digitale Perfektionierung sozialer Kontrolle der Bürger im Reich der Mitte ihren Lauf.

(2) Digitale Polizeiarbeit

Polizeibehörden nutzen soziale Netzwerke inzwischen insbesondere als Gefahrenradar und Verdachtssensorium.[45] Sie durchsuchen deren Datenpanoramen im Rahmen einer automatisierten Online-Streife, insbesondere um rechtswidrige Inhalte aufzuspüren oder Anhaltspunkte für die Verfolgung von Straftätern zu erhaschen.[46] Die Polizei macht sich dabei eine Eigenheit des Cyberspace zunutze: Die Grenze zwischen privatem und öffentlichem Raum ist im digitalen Kosmos – anders als in der Offline-Welt – fließend. Die Bevölkerung füttert das Web 2.0 freimütig mit privaten heiklen Fakten, ohne sich ihrer Beobachtung durch staatliche Behörden immer bewusst zu sein. Je größer der Datenfundus wird, umso tiefgreifender und ertragreicher die Recherche. So gelten die sozialen Netzwerke inzwischen als Fundgruben für allgemeine Ermittlungs- und Fahndungszwecke sowie präventionspolizeiliche Maßnahmen.[47]

II. Verfassungsrechtlicher Handlungsrahmen

Nicht jede Erscheinungsform des Social Media Monitorings ist verfassungsrechtlich sensibel. Persönlichkeitssensitiv ist aber (auch bei der Aggregierung von Massendaten zu Auswertungszwecken) die Erhebung der Daten aus sozialen Netzwerken, um sie in den Topf der Datenauswertung eines Social Media Monitorings zu geben. Erst recht kann ein ad personam erfolgendes Social Media Monitoring, welches gezielt nach dem Verhalten von Einzelpersonen fahndet, das verfassungsrechtlich geschützte informationelle Selbstbestimmungsrecht tangieren.

1. Grundsatz: Grundrechtliche Vorbehaltsfreiheit einer Auswertung allgemein zugänglicher Quellen

Wer sich in die Öffentlichkeit begibt, entledigt sich dadurch nicht des Rechts, selbst zu bestimmen, innerhalb welcher Grenzen persönliche Sachverhalte offenbart und (weiter-)verwendet werden. Indem er Informationen im Internet preisgibt, macht der Einzelne vielmehr von dieser Freiheit zur

---

[45] Zu den Rahmenbedingungen der Online-Ermittlung durch BKA und Polizeibehörden de lege lata bereits oben Fußn. 7.
[46] Siehe hierzu *Meinecke*, Big Data und Data Mining: Automatisierte Strafverfolgung als neue Wunderwaffe der Verbrechensbekämpfung?, in: Taeger (Hrsg.), Big Data & Co, 2014, S. 183. Vgl. auch *Beuth*, Das BKA will in die Zukunft sehen, Zeit Online vom 17.3.2014; die Aussagen der Bundesregierung in BT-Drucks. 18/2932, S. 12 f. sowie *Oermann/Staben* (Fn. 14), 630 f. Vgl. auch *Schulz/Hoffmann* (Fn. 11), Rdnr. 62 ff. sowie *Schulz/Hoffmann*, DuD 2012, 7 ff.
[47] *Henrichs/Wilhelm* (Fn. 3), 30. Auf eine systematische und anlasslose Recherche setzten Bundeskriminalamt, Bundespolizei und Zollfahndungsdienst jedoch jedenfalls im Jahr 2011 noch nicht – so die Antwort der Bundesregierung auf die Kleine Anfrage „Nutzung sozialer Netzwerke zu Fahndungszwecken“, BT-Drucks. 17/6587, S. 2.

Selbstdarstellung in spezifischer Weise Gebrauch:[48] Er entfaltet sein Recht zur Selbstbestimmung, indem er andere an seiner Privatheit teilhaben lässt. Dass persönliche Informationen in sozialen Netzwerken einem weiten Kreis an Personen ohne größere Beschränkung zugänglich sind,[49] lässt den grundrechtlichen Persönlichkeitsschutz der von der Auswertung Betroffenen daher zwar nicht entfallen.[50] Wenn staatliche Stellen jedermann zugängliche, also internetöffentliche Informationen anmeldefrei wahrnehmen und auswerten, greift das aber noch nicht per se in das informationelle Selbstbestimmungsrecht ein.[51] Denn derjenige, der die allgemeine Öffentlichkeit sucht, gibt zu erkennen, dass er eine Information nicht für vollumfänglich vertraulich hält und mit dem Zugriff auf die Daten durch Dritte einverstanden, sie insbesondere mit einem unbestimmten Personenkreis zu teilen bereit ist.[52] Wer sich dann gegenüber Dritten auf die Privatheit der Information beruft, setzt sich zum eigenen Verhalten in Widerspruch. Entsprechend bedürfen auch in der analogen Welt die bloße Streifenfahrt als allgemeine vorbehaltsfreie Aufklärungsmaßnahme und das Nachschlagen in einem Telefonbuch grundsätzlich keiner besonderen Rechtsgrundlage.[53]

2. Grenzen und Ausnahmen

Dass die Wahrnehmung allgemein zugänglicher Quellen grundrechtlich grundsätzlich keiner Eingriffsgrundlage bedarf, heißt aber noch nicht, dass jegliche Form der Online-Streife, also die Beobachtung öffentlicher Privatheit im Internet, ausnahmslos jedes grundrechtlichen Rechtfertigungsbedarfs enthoben ist.[54] Nicht nur hat der Betroffene nicht zwingend alles, was der Öffentlichkeit zugänglich ist, unbedingt selbst ins Internet eingespeist. Vor allem impliziert die Verbreitung einer Nachricht an die Gemeinschaft eines sozialen Netzwerks (Netzwerköffentlichkeit) noch nicht, dass die Person auch mit einer Kenntnisnahme der allgemeinen (Internet-)

---

[48] BVerfG (1. Kammer des Ersten Senats), Beschluss vom 23.2.2007, NVwZ 2007, 688 (690); BVerfG, Urteil vom 11.3.2008, BVerfGE 120, 378 (399, Rdnr. 67); *Schulz/Hoffmann*, CR 2010, 131 (134).

[49] Private können sich für die Verarbeitung der öffentlich zugänglichen Daten sozialer Netzwerke gegenüber dem Staat dann auf die grundrechtliche Verbürgung der Informationsfreiheit, also des Rechts, sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten, berufen.

[50] Etwas zu weitgehend daher BVerfGE 78, 38 (51).

[51] *Bäcker*, Der Staat 2012, 91 (103 f.); *Oermann/Staben* (Fn. 14), 638 (unter Berufung auf BVerfGE 120, 274 [344], wenngleich sich die Aussage dem Urteil nicht entnehmen lässt; die Äußerungen des BVerfG beziehen sich vielmehr auf die Vertraulichkeit und Integrität informationstechnischer Systeme); *Schulz/Hoffmann* (Fn. 11), Rdnr. 64. Anders liegt dies in den Fällen der Überwachung außerhalb der Wohnung, so z. B. längerfristiger Observation und der Erstellung heimlicher Bildaufzeichnungen, wie sie § 20g Abs. 1 BKAG vorsieht. Das BVerfG erkennt darin jedenfalls einen Eingriff geringer Intensität in das Recht auf informationelle Selbstbestimmung; BVerfG, Urteil vom 20.4.2016, NJW 2016, 1781 (1789, Rdnr. 147, 149 ff.).

[52] BVerfG, Urteil vom 27.2.2008, BVerfGE 120, 274 (344 f.).

[53] *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 512. Dieser Analogie widersprechen *Schulz/Hoffmann* (Fn. 46), 134.

[54] In diesem Sinne aber wohl *Germann* (Fn. 51), S. 512.

Öffentlichkeit, jedes Dritten, insbesondere staatlicher Stellen, sowie jeder Form der Weiterverarbeitung und Verschneidung mit anderen Daten einverstanden ist.[55]

a) Inanspruchnahme persönlichen Vertrauens in die Kommunikationsbeziehung

Nach dem konzeptionellen Zuschnitt des Rechts auf informationelle Selbstbestimmung reicht das Einverständnis zur Auswertung von Informationen nur so weit, wie der Grundrechtsträger es erteilt hat. Er kann es auch selektiv erteilen, z. B. auf bestimmte Personen beschränken.[56] Die Limitierung der Reichweite muss dann allerdings hinreichend klar zum Ausdruck kommen. Denn ein Vertrauen in den Schutz vor einem Zugriff Dritter kann nur geltend machen, wer zu erkennen gibt, dass seine durch Verlautbarung gelebte öffentliche Privatheit ausschließlich die Wahrnehmung durch bestimmte oder in bestimmter Weise qualifizierte Dritte einschließt – indem er etwa als Nutzer sozialer Netzwerke die Datenschutzvoreinstellung entsprechend konfiguriert oder Inhalte nur für einen bestimmten geschlossenen Benutzerkreis veröffentlicht. Missbraucht der Staat in einem solchen Fall das schutzwürdige Vertrauen des Betroffenen in die Integrität seines Kommunikationspartners, greift er in das Recht auf informationelle Selbstbestimmung ein.[57]

Nimmt die verlautbarte Information demgegenüber, sei es bei einer Meinungskundgabe innerhalb einer sehr großen Gruppe, sei es im Rahmen einer Individualkommunikation, kein schutzwürdiges (z. B. durch eine Identitätsprüfung [58] sichergestelltes) Vertrauen in die Identität des Kommunikationspartners in Anspruch, bedarf die staatliche Beobachtung grundsätzlich keiner Eingriffsgrundlage.

Regelmäßig ist jedem Kommunikationspartner im Rahmen einer Kommunikationsbeziehung im Cyberspace bewusst, „dass er die Identität seiner Partner nicht kennt oder deren Angaben über sie jedenfalls nicht überprüfen kann“[59]. Die notwendige Individualisierung des Gegenübers lässt sich dann nicht herstellen; auch E-Mail-Adressen vermitteln (mit Ausnahme z. B. der De-Mail) grundsätzlich keine absolute Identitätssicherheit.[60] Das Vertrauen des Einzelnen darauf, dass er

---

[55] *Schulz/Hoffmann* (Fn. 44), 10.

[56] Dem Nutzer sind je nach Netzwerk eine Vielzahl von Kommunikationsformen eröffnet, bei denen jeweils im Einzelfall die Frage zu beantworten ist, wie sich der beabsichtigte Adressatenkreis bestimmt. Bei Facebook etwa kann der Nutzer mit einer oder mehreren Personen Nachrichten austauschen bzw. chatten, Informationen in Gruppen posten, die ihrerseits durch eigene Zugangshürden gesichert sein können; er kann aber auch die Sichtbarkeit der jeweils geposteten Information, auch im Profil oder der „Timeline“, individuell regulieren.

[57] BVerfG, Urteil vom 27.2.2008, BVerfGE 120, 274 (345, Rdnr. 310). Zur Bedeutung des Vertrauensschutzes in die Achtung von Zugangshürden als Voraussetzung für die grundrechtliche Entfaltung von Privatheit im Internet ausführlich *Eichenhofer*, Der Staat 55 (2016), 41 (50 ff.).

[58] *Schulz/Hoffmann* (Fn. 46), 132.

[59] BVerfG, Urteil vom 27.2.2008, BVerfGE 120, 274 (346, Rdnr. 311).

[60] *Böckenförde*, Die Ermittlung im Netz, 2003, S. 198.

nicht mit einer staatlichen Stelle kommuniziert, ist daher nach Einschätzung des BVerfG grundsätzlich nicht schutzwürdig und damit z. B. bei der Teilhabe an der Kommunikation eines anonymen Internetforums unter Pseudonym eine Eingriffsgrundlage nicht erforderlich.

Diese Wertung überzeugt nicht vollständig. Selbst wenn die Identität des Gegenübers nicht überprüfbar ist, darf der Betroffene jedenfalls im Rahmen einer Individualkommunikation grundsätzlich darauf vertrauen, dass sein Kommunikationspartner, z. B. im Rahmen eines Facebook-Chats oder bei einer Kontaktaufnahme via Tinder, nicht im Auftrag einer Sicherheitsbehörde handelt und seine Vertrauenserwartung, mit einer Privatperson zu kommunizieren, nicht enttäuscht.[61] Müsste der Einzelne stets damit rechnen, dass sich hinter Internetprofilen natürlicher Personen der Staat als Akteur verbirgt, der verdachtsunabhängig unter einer Legende ermittelt (sei es als Verdeckter Ermittler unter Ausnutzung eines gefälschten Profils, sei es als V-Mann, der unter Wahrung seiner Identität die Daten als Vertrauensperson für die Polizei in sozialen Netzwerken erhebt), ginge davon eine nachhaltig abschreckende Wirkung für die Entfaltung der Meinungsfreiheit und des individuellen Selbstentwurfs in einer freiheitlichen Gesellschaft aus.[62] Das Einverständnis zur Kommunikation bezieht sich bei personengebundener, etwa via Chat erfolgender Kommunikation, in der Regel nur auf diejenige natürliche Person, die vorgeblich hinter der Online-Identität steckt – nicht auf jeden, der dieses Profil nutzt oder nutzen kann.[63] Den Staat trifft insbesondere eine verfassungsrechtliche Neutralitätspflicht, seine Kommunikation in gesellschaftlichen Kommunikationssphären „mit offenem Visier“ zu betreiben.[64] Soll eine solche Form der Internetaufklärung verdeckt erfolgen, bedarf dies einer hinreichend klaren Eingriffsgrundlage – zwar nicht zwingend mit Blick auf Art. 20 Abs. 3 GG, sehr wohl aber sub specie des informationellen Selbstbestimmungsrechts.[65] Das gilt vor allem in besonders geschützten Bereichen, etwa der Ausübung der Religionsfreiheit (Art. 4 Abs. 1, 2 GG), der Versammlungs- und Vereinigungsfreiheit (Art. 8 Abs. 1 und 9 Abs. 1 GG) oder in familiären Angelegenheiten (Art. 6 GG),

---

[61] In diese Richtung auch *Biemann* (Fn. 7), S. 124, 146 m. w. N.; *Eifert*, NVwZ 2008, 521 (522); *Hornung*, CR 2008, 299 (305); *Schulz/Hoffmann* (Fn. 44), 12.

[62] *Grabenwarter*, in: Maunz/Dürig (Hrsg.), GG, 75. Erglfg. (Sept. 2015), Art. 5, Rdnr. 104.

[63] *Schulz/Hoffmann* (Fn. 44), 12.

[64] *Eifert*, Verwaltungskommunikation im Internet, in: Ladeur (Hrsg.), Innovationsoffene Regulierung des Internet, 2003, S. 131 (146); *Eifert* (Fn. 59), 522. Dem trägt beispielsweise die Transparenzpflicht des § 6b Abs. 2 BDSG bei der Videoüberwachung in konsequenter Weise Rechnung.

[65] Das Telekommunikationsgeheimnis schützt nicht das personengebundene, sondern nur das mediengebundene Vertrauen der Kommunikationsbeteiligten zueinander, die Privatheit auf Distanz; BVerfG, Beschluss vom 9.10.2002, BVerfGE 106, 28 (35 ff., Rdnr. 19 ff.); *Schulz/Hoffmann* (Fn. 46), 133. Ein Eingriff in Art. 10 GG liegt aber dann vor, wenn die Kommunikation auf einem technisch nicht vorgesehenen Weg erhoben wird, z. B. wenn die Polizei ein mittels Keylogging erhobenes Passwort einsetzt, um Zugang zu einem E-Mail-Postfach und zu angeschlossenen Chats zu erlangen oder wenn es an einer Autorisierung fehlt, also einer der Kommunikationspartner der Verwendung der Daten nicht zustimmt, *Schulz/Hoffmann* (Fn. 44), 13.

sowie allgemein dort, wo die Kommunikation über Daten, die dem Kernbereich privater Lebensgestaltung besonders nahe stehen, wahrscheinlich ist. [66] Das informationelle Selbstbestimmungsrecht versteht sich in seiner Schutzfunktion insoweit auch als Vorfeldgrundrecht für die Ausübung anderer grundrechtlicher Betätigungen. Die allgemeinen Rechtsgrundlagen [67] reichen dann regelmäßig nicht aus, um Eingriffe verfassungsrechtlich zu legitimieren.

Greift der Staat auf Informationen zu, die personengebundenes Vertrauen in die Kommunikationsbeziehung in Anspruch nehmen, [68] beispielsweise bei der staatlichen Fahndung unter einem falschen Facebook-Profilnamen, bedarf er daher einer besonderen Eingriffsgrundlage.[69]

b) Systematische staatliche Zusammenführung allgemein zugänglicher Quellen zu einem Persönlichkeitsprofil

Einer Eingriffsgrundlage bedarf es auch dann, wenn staatliche Stellen allgemein zugängliche Inhalte gezielt zusammentragen, speichern und (ggf. unter Hinzuziehung weiterer Daten) ad personam auswerten[70] – etwa, wenn Mitarbeiter in Jobcentern Informationen aus sozialen Netzwerken (und eigenen Datenbanken) miteinander verschneiden, um aus einem Monitoring auf die Lebensbedingungen, Einkommens- und Beschäftigungsverhältnisse der Leistungsempfänger zu schließen. Denn aus der Komposition einzelner, ansonsten inkonnexer Informationen zu einem Gesamtbild erwächst eine besondere Gefahrenlage für die individuelle Selbstentfaltung, die den Kerngehalt des Allgemeinen Persönlichkeitsrechts beeinträchtigt. Eine solche Form der Beobachtung wirkt insbesondere auf die Ausübung von Kommunikationsbeziehungen und damit mittelbar auch auf die Meinungsfreiheit in eingriffsäquivalenter Weise abschreckend ein. Der Einzelne ist durch die Beobachtungswirkung staatlichen Kontrollverhaltens dem Odium ständigen

---

[66] BVerfG, Urteil vom 20.4.2016, NJW 2016, 1781 (1783, Rdnr. 94); *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, 2007, S. 48 ff.

[67] Insbesondere § 161 Abs. 1, § 163 Abs. 1 und § 110a Abs. 1 Satz 1 StPO für die repressive Aufgabenwahrnehmung; für die präventive Tätigkeit insbesondere die polizeirechtlichen Datenverarbeitungsgrundlagen, namentlich beispielsweise Art. 30 BayPAG; § 26 RhPfPOG; § 2 Abs. 2 Satz 1, Abs. 3 Satz 1 HmbPolDVG. Dazu auch Fußn. 7 sowie bspw. *Bär*, MMR 1998, 463 (465 ff.) sowie *Germann* (Fn. 51), S. 503 ff u. 523 ff.

[68] Das kann sich nicht nur im Rahmen eines Individualchats einstellen, sondern auch bei einer Chatgruppe in einem kleineren Kreis, im Einzelfall sogar bei einer Information an eine größere Personengruppe, sofern sich hier jeweils eine persönliche Vertrauensbeziehung manifestiert hat.

[69] Das Land Nordrhein-Westfalen hat mit § 5 Abs. 2 Nr. 11 VSG NRW eine solche Eingriffsgrundlage geschaffen für den „Zugriff auf zugangsgesicherte Telekommunikationsinhalte und sonstige Informations- und Kommunikationsinhalte im Internet auf dem technisch hierfür für jede Nutzerin und jeden Nutzer vorgesehenen Weg, ohne selbst Kommunikationsadressatin oder -adressat und ohne von den an der Kommunikation teilnehmenden Personen oder vergleichbaren Berechtigten hierzu autorisiert zu sein (…)“.

[70] BVerfG, Urteil vom 27.2.2008, BVerfGE 120, 274 (345, Rdnr. 309); BVerfG, Urteil vom 11.3.2008, BVerfGE 120, 378 (398 f., Rdnr. 66); BVerwG, Urteil vom 21.7.2010, BVerwGE 137, 275 (279, Rdnr. 17); *Biemann* (Fn. 7), S. 132 f.

Überwachtwerdens ausgesetzt und richtet sein Verhalten daran im Zweifel aus.[71] Gerade vor solchen „chilling effects" will das informationelle Selbstbestimmungsrecht den Einzelnen bewahren. Eine Dauerbeobachtung des privaten und gesellschaftlichen Lebens vermittelt dem Staat nämlich beherrschenden Kontrolleinfluss auf Teile der privaten und öffentlichen Meinungsbildung.[72] Der dadurch bedrohte bürgerliche Freiheitsbereich ist aber Funktionsbedingung für die Entfaltung eines demokratischen Gemeinwesens. Social Media Monitoring in Gestalt einer Zusammenführung inkonnexer Daten zu Persönlichkeitsprofilen und der systematischen Beobachtung privater Lebenssachverhalte ist deswegen grundsätzlich nur auf der Grundlage einer gesetzlichen Eingriffsermächtigung zulässig.

III. Einfachgesetzliche Zulässigkeit

Das einfachgesetzliche Recht hält zahlreiche Grundlagen für den Zugriff auf Daten vor, die für ein Social Media Monitoring Verwendung finden – insbesondere im TKG, im TMG und im BDSG.

Für die Erhebung, Verarbeitung und Nutzung von *Telekommunikationsdaten*, insbesondere Standortdaten, steckt das TKG (insbesondere in § 96 Abs. 1 Satz 1 Nr. 5, § 96 Abs. 1 Satz 2, § 96 Abs. 3 und § 98 TKG)[73] den Zulässigkeitsrahmen ab. Ausweislich seines § 91 Abs. 1 Satz 1 erstreckt es seinen Geltungsanspruch aber nur auf Telekommunikationsdiensteanbieter. In dieser Funktion tritt der Staat dem Einzelnen beim Social Media Monitoring indes nicht gegenüber; das TKG findet auf ihn nur ausnahmsweise Anwendung, wenn er – sei es als Anbieter eines Dienstes mit Zusatznutzen (§ 98 Abs. 1 Satz 4 TKG), sei es im Rahmen der Telekommunikationsüberwachung (§ 100a StPO) – auf Telekommunikationsdaten zugreift.

Den zulässigen Zugriff auf *Nutzungsdaten*, wie Verweildauer und Zeitpunkt des Aufrufes einer Internetseite, grenzt das TMG ein – insbesondere in § 15 Abs. 1[74] und Abs. 3 Satz 1: Der Diensteanbieter darf zwar unter Verwendung von Pseudonymen *Nutzungs*profile erstellen, nicht jedoch für jede erdenkliche Zielsetzung, sondern nur für Zwecke der Werbung, Marktforschung oder bedarfsgerechten Gestaltung seiner Telemedien. Als Abfallprodukt seines Dienstangebots

---

[71] Das BVerfG spricht von der „diffusen Bedrohlichkeit geheimer staatlicher Beobachtung" (BVerfG, Urteil vom 20.4.2016, NJW 2016, 1781 [1788, Rdnr. 132]), der EuGH vom „Gefühl", dass das „Privatleben Gegenstand einer ständigen Überwachung" ist (EuGH, Urteil vom 8.4.2014 – Digital Rights Ireland Ltd. –, ECLI:EU:C:2014:238, Rdnr. 37). Neuere empirische Erkenntnisse – aufgezeigt am Beispiel der NSA-Überwachung – stützten die These, dass Internetnutzer ihr Verhalten beim Verdacht möglicher staatlicher Überwachung anpassen; vgl. *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, 2015; *Penney*, Berkeley Technology Law Journal 31 (2016), 117, 1.

[72] Vgl. auch BVerfG, Urteil vom 22.2.1994, BVerfGE 90, 60 (88 f.).

[73] Zur Abgrenzung zwischen § 96 Abs. 1 Satz 1 und § 98 Abs. 1 TKG *Martini/Weiß/Ziekow*, Rechtliche Zulässigkeit flächendeckender Alarmierungen der Bevölkerung in Katastrophenfällen per SMS (KatWarn), 2013, S. 95 ff.

[74] Zu seiner (Un-)Vereinbarkeit mit dem Unionsrecht jüngst Schlussanträge des GA *Sánchez* vom 12.5.2016 in der Rs. C-582/14, Rdnr. 93 ff.

*Persönlichkeits*profile zu generieren, ist ihm demgegenüber verwehrt. Das TMG verbietet auch ausdrücklich, Nutzerdaten mit anderen Daten über den Nutzer (außer für Abrechnungszwecke – § 15 Abs. 2 TMG) zu einem neuen Datensubstrat zusammenzuführen (§ 15 Abs. 3 Satz 3 TMG). Das gilt – wie § 1 Satz 2 TMG klarstellt – nicht nur für Private, sondern auch für öffentliche Stellen; das TMG ist auf sie jedoch nur anwendbar, wenn sie, wie z. B. im Falle des Betriebs eines Partizipationsportals, selbst Diensteanbieter sind.[75]

Soweit sich Social Media Monitoring – wie typischerweise – auf den *Inhalt* der Kommunikation als Auswertungsressource erstreckt, z. B. die Tonalität einer Unterhaltung oder bestimmte Signalwörter, zieht das BDSG bzw. in Zukunft die DSGVO[76] den Rahmen. Das Datenschutzregime stellt die Auswertung der Inhalte sozialer Netzwerke unter einen Rechtfertigungsvorbehalt:[77] Erforderlich ist entweder eine informierte Einwilligung oder eine gesetzliche Verarbeitungserlaubnis (§ 4 BDSG;[78] Art. 6 Abs. 1 DSGVO[79]). Das Verbotsprinzip des Datenschutzrechts erfasst aber nur personenbezogene Daten (vgl. § 3 Abs. 1 BDSG[80]; Art. 4 Nr. 1 DSGVO). Solche sind jedenfalls betroffen, wenn Social Media Monitoring mit klarnamengeprägten Netzwerkprofilen[81] operiert, die Rückschlüsse auf bestimmte Personen erzielen sollen, um Gesetzesverstößen auf die Spur zu kommen; etwa bei Ermittlungen der Steuer-, Sozial- und Polizeibehörden auf Facebook-Seiten, Twitter- oder Blogeinträgen.

Soweit sich die Monitoring-Auswertung demgegenüber auf anonymisierte Inhaltsdaten beschränkt, die keinen Rückschluss auf bestimmbare Personen zulassen (§ 3 Abs. 6 BDSG[82]), so etwa

---

[75] Auf Anordnung dürfen sich aber auch Sicherheitsbehörden im Einzelfall Zugriff auf Nutzungsdaten verschaffen (§ 15 Abs. 4 Satz 4 i. V. mit § 14 Abs. 2 TMG). Dazu kritisch bspw. *Karg*, DuD 2015, 85 (87 f.). Zur Verantwortungszurechnung zwischen einem Diensteanbieter und öffentlichen Stellen, insbesondere zur Auftragsdatenverarbeitung, wenn sie sich die Auswertungsdienste Dritter, z. B. Facebook Insights oder anderer Monitoring-Tools nutzbar machen, siehe *Eckhardt/Kramer*, DuD 2016, 144 ff.; *Martini/Fritzsche* (Fn. 8), 2 ff.

[76] Im Hinblick auf elektronische Kommunikationsdienste im Sinne des TMG genießen die Regelungen der Richtlinie 2002/58/EG grundsätzlich Vorrang (Art. 95 DSGVO). Für die Datenverarbeitung eines Social Media Monitorings im Rahmen der Strafjustiz und Polizei – und damit einen erheblichen Teil des denkbaren Anwendungsbereichs öffentlicher Stellen – setzen künftig die allgemein gehaltenen Rahmenvorgaben der Richtlinie 2016/680/EU vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. EU L 119 vom 27.4.2016, S. 89 ff., die äußeren Grenzen, die allerdings im nationalen Recht nur geringen Anpassungsbedarf auslösen.

[77] Das einfache Recht schießt insoweit über die verfassungsrechtlichen Schutzerfordernisse des informationellen Selbstbestimmungsrechts (dazu oben II. 1., S. 16) hinaus.

[78] Für die landesrechtlichen Datenschutzgesetze pars pro toto § 4 Abs. 1 Satz 1 NRWDSG.

[79] Für die Verarbeitung personenbezogener Daten zu präventiv- bzw. repressiv-polizeilichen Zwecken: Art. 8 Abs. 2 Richtlinie 2016/680/EU (Fußn. 76).

[80] Die landesrechtlichen Datenschutzgesetze enthalten weitgehend identische Definitionen, so z. B. § 3 Abs. 1 NRWDSG.

[81] Dazu zählen etwa Facebook (vgl. Punkt 4 der Nutzungsbedingungen) und Xing (vgl. Punkt 4.1. lit a der AGB).

[82] Die DSGVO legt eine ähnliche Definition anonymer Daten zugrunde (ErwGrd 26 DGSVO). Mit Ausnahme Hessens und Niedersachsens enthalten die landesrechtlichen Datenschutzgesetze mit § 3 Abs. 6 BDSG vergleichbare Definitionen.

typischerweise bei allgemeiner Stimmungserkundung und Trendanalyse zur politischen Steuerung,[83] ist der Anwendungsbereich des Datenschutzrechts nur bei der Filterung personenbezogener Daten aus dem Datenbestand[84] eröffnet. Der Wert solcher Beobachtungen liegt nicht in der ad personam erfolgenden Inhaltsauswertung, sondern der Aggregierung von Metadaten für überblicksartige Einschätzungen. Die Verarbeitung (§ 3 Abs. 4 BDSG) solcher anonymisierter Daten ist dann nicht datenschutzrechtlich rechtfertigungsbedürftig,[85] sehr wohl aber deren Erhebung (§ 3 Abs. 3 BDSG), solange sie noch personenbezogen sind.

1. Einwilligung

Die Einwilligung des Betroffenen ist die persönlichkeitsfreundliche „Goldrandlösung" eines Social Media Monitorings. Die bloße Anmeldung und Teilnahme an einem sozialen Netzwerk genügt dafür grundsätzlich noch nicht.[86] Der Nutzer sozialer Netzwerke erteilt zwar eine Einwilligung in die Nutzung seiner Daten. Diese umfasst allerdings nicht die Auswertung der Informationen *durch jedermann*, insbesondere durch staatliche Stellen, sondern wirkt grundsätzlich ausschließlich in dem Innenverhältnis zu dem Diensteanbieter: Nur Facebook & Co. sind Adressaten einer Einwilligung ihrer Nutzer; Dritten verleiht sie keine Verarbeitungsgrundlage. Dieser konzeptionelle Wille des Gesetzgebers ergibt sich mittelbar auch daraus, dass er an verschiedenen Stellen – insbesondere in § 13 Abs. 2 Nr. 2 und 4 BDSG – die Einwilligung als selbstständige Verarbeitungsgrundlage neben die öffentliche Bekanntmachung des Betroffenen stellt. Läge in der selbstbestimmten Verbreitung einer Information an die Allgemeinheit bereits eine Einwilligung, hätte es einer zusätzlichen Verankerung dieser gesetzlichen Verarbeitungsgrundlage nicht bedurft. Die Einwilligung im Sinne des einfachen Datenschutzrechts reicht zudem (anders als die

---

[83] Zum Personenbezug von IP-Adressen Art. 4 Nr. 1 Hs. 2 DSGVO; BGH, ZD 2015, 80 ff.; GA *Sánchez* (Fußn. 74), Rdnr. 52 ff.; *Martini*, NVwZ-Extra 3/2016, 1 (3 f.).

[84] Denn das Beschaffen der Informationen knüpft an personenbezogene Profile an, so dass der Verbotsvorbehalt des § 4 BDSG (bzw. seine landesrechtlichen Äquivalente) und in Zukunft Art. 6 Abs. 1 DSGVO greift. Siehe dazu auch Fußn. 114 u. 128 sowie *Hornung*, Datenschutzrechtliche Aspekte der Social Media, in: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2015, Rdnr. 101.

[85] Anders liegt es nur, wenn zwar kein unmittelbarer Personenbezug mehr besteht, unter Big- Data-Bedingungen entstehende Zusammenführungs-, Rückverfolgungs- und Analysemöglichkeiten jedoch die reindividualisierende Zuordnung eines Social Media-Beitrages bzw. der darin mitgeteilten Informationen zu einer bestimmten Person ermöglichen. Eine von dem Klammergriff des Datenschutzrechts befreiende Anonymisierung schließt das aus. *Koch*, ITRB 2015, 13 (18). Ähnlich auch *Baeriswyl*, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber/Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, 2014, S. 51 (51 f.); illustrativ auch *Bohannon*, science 347 (2015), 468 (468).

[86] A. A. wohl *Schulz*, Einsatz von Social Media durch die öffentliche Verwaltung, in: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2015, Rdnr. 98.

verfassungsrechtliche Einwilligung) nur so weit, wie sie den Zweck der Auswertung hinreichend klar benennt (§ 13 Abs. 2 Nr. 1 TMG; § 4a Abs. 1 Satz 1 BDSG[87]; Art. 7 Abs. 2 DSGVO).[88]

Ermächtigt der Diensteanbieter in Allgemeinen Nutzungsbedingungen *Dritte* zur Auswertung des Kommunikationsinhalts, insbesondere zur Herauslösung der Daten aus dem Verwendungskontext, handelt es sich dabei regelmäßig um eine überraschende Klausel, die den Betroffenen entgegen den Geboten von Treu und Glauben[89] unangemessen benachteiligt und damit nach § 307 Abs. 1 Satz 2 und Abs. 2 Nr. 1 BGB unwirksam ist. Das gilt insbesondere dann, wenn die Identität der Dritten oder die Zielrichtung ihrer Auswertung nicht klar erkennbar ist und folglich eine Abweichung von dem Leitbild gesetzlicher Bestimmungen vorliegt. [90] Wer einen Text in den durch Authentifizierungserfordernisse geschützten Bereich sozialer Netzwerke einstellt, geht in der Regel nicht davon aus, dass jedermann diese Inhalte auswerten und verwerten darf (und wird).[91] Der Äußernde willigt mit der Verbreitung einer nur nach Autorisierung zugänglichen Nachricht auch nicht stillschweigend in ihre Auswertung durch unbekannte Dritte oder staatliche Stelle ein. Der Zweck der Verarbeitung muss dem Einwilligenden stets bekannt sein (§ 4a Abs. 1 Satz 2 BDSG).

2. Gesetzliche Verarbeitungserlaubnis

Ist ein Social Media Monitoring auch regelmäßig nicht von einer Einwilligung der Betroffenen gedeckt, eröffnen die Datenschutzgesetze ihm doch in weitem Umfang eine Verarbeitungsgrundlage. Für allgemein zugängliche Quellen gestehen sie verantwortlichen Stellen ein Auswertungs- und Nutzungsprivileg zu. Sie dürfen die in allgemein zugänglichen Quellen hinterlegten Informationen grundsätzlich verarbeiten.[92]

Nicht-öffentliche Stellen privilegiert das Gesetz vorbehaltlos – sowohl bei der Nutzung für eigene Geschäftszwecke (§ 28 Abs. 1 Satz 1 Nr. 3 BDSG), bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung (§ 29 Abs. 1 Satz 1 Nr. 2 BDSG) als auch bei der geschäftsmäßigen Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung (§ 30a Abs. 1

[87] So auch für das Landesrecht etwa § 6 Abs. 5 BlnDSG; § 3 Abs. 3 BremDSG; § 5 Abs. 2 HmbDSG; § 4 Abs. 3 NdsDSG; § 4 Abs. 1 NRWDSG und § 5 Abs. 2 RhPfLDSG.

[88] Dazu auch *Zimmermann*, Die Einwilligung im Internet, 2014, S. 260 ff.

[89] Art. 5 Abs. 1 lit. a DSGVO erklärt (in Fortführung des Art. 6 Abs. 1 lit. a RL 95/46/EG) den Grundsatz von Treu und Glauben in Zukunft für die Rechtmäßigkeit der Datenverarbeitung für unmittelbar anwendbar.

[90] Dazu wegweisend LG Berlin, Urteil vom 30.4.2013, NJW 2013, 2605 (2607), das die Datenschutzbedingungen von Apple als AGB eingestuft und für unwirksam erklärt hat. Siehe auch LG Frankfurt a. M., Urteil vom 6.6.2013, MMR 2013, 645 (646 f.).

[91] *Schreiber* (Fn. 12), 35; *Solmecke/Wahlers* (Fn. 22), 552.

[92] Die DSGVO enthält keine spezielle Verarbeitungsgrundlage für allgemein zugängliche Daten, erachtet deren Verarbeitung aber wohl als zulässig. Dazu im Einzelnen unten IV., S. 44.

Satz 1 Nr. 2 BDSG[93]).[94] Das gilt auch im Arbeitsverhältnis, insbesondere beim Bewerbermonitoring: § 28 Abs. 1 Nr. 3 BDSG ist insoweit nicht durch die Sondernorm des § 32 BDSG gesperrt.[95]

Das Auswertungs- und Nutzungsprivileg nicht-öffentlicher Stellen für allgemein zugängliche Quellen ist Ausfluss der verfassungsrechtlich verbürgten Informationsfreiheit (Art. 5 Abs. 1 Satz 1 Hs. 2 GG):[96] Das Recht, sich aus allgemein zugänglichen Quellen zu unterrichten, bedingt grundsätzlich die datenschutzrechtliche Verarbeitungsbefugnis. Wessen Daten jedermann zugänglich sind, muss auch damit rechnen, dass auch unbekannte Dritte sie wahrnehmen und nutzen.[97]

Für *öffentliche Stellen* schwächt das Gesetz die Privilegierung hingegen deutlich ab. Das ist auch konsequent. Denn anders als Private sind öffentliche Stellen umfassend grundrechtlich gebunden; sie handeln nicht in Ausübung grundrechtlicher Informationsfreiheit, sondern als Treuhänder bürgerlicher Freiheitsrechte. Den rechtlichen Rahmen für ihre Social Media Monitoring-Maßnahmen ziehen die Vorschriften des § 13 Abs. 1, 14 Abs. 1, Abs. 2 Nr. 5 BDSG bzw. ihre landesrechtlichen Äquivalente[98]. Sie begrenzen das Monitoring – normativ strukturell ähnlich wie die Videobeobachtung öffentlich zugänglicher Räume nach § 6b Abs. 1 Nr. 1 und Abs. 3 BDSG – auf das zur Erfüllung öffentlicher Aufgaben Erforderliche (a und b), befreien aber immerhin von der Bindung an die Zwecke, für welche die Daten ursprünglich erhoben worden sind (c).

Bremen, Hamburg, Hessen und Rheinland-Pfalz [99] nehmen die Datenverarbeitung allgemein zugänglicher personenbezogener Daten durch öffentliche Stellen sogar insgesamt aus dem

---

[93] Zur Abgrenzung zwischen § 28 und § 30a BDSG siehe bspw. *Ehmann*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 30a, Rdnr. 33 ff.; *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl., 2013, § 30a BDSG, Rdnr. 5 ff.

[94] Es gelten insoweit jeweils grundsätzlich die gleichen Maßstäbe. Vgl. *Ehmann* (Fn. 91), § 30a, Rdnr. 122; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 30a, Rdnr. 4; *Kramer*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 29 BDSG, Rdnr. 36 sowie § 30a Rdnr. 18.

[95] Denn § 28 Abs. 1 Satz 1 Nr. 3 BDSG setzt kein Vertragsverhältnis voraus. Entsprechend erwähnt die Gesetzesbegründung zu § 32 BDSG als verdrängte Vorschriften konsequenterweise nur § 28 Abs. 1 Satz 1 Nr. 1 BDSG und § 28 Abs. 1 Satz 2 BDSG, nicht aber § 28 Abs. 1 Satz 1 Nr. 3 BDSG (BT-Drucks. 16/13657, S. 20). § 32 BDSG ist im Verhältnis zu dieser Norm also nicht Lex specialis. Siehe dazu auch *Hornung* (Fn. 82), Rdnr. 104; *Solmecke*, Teil 21.1 - Social Media, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, 43. Erg.-Lfg., 2016, Rdnr. 45; *Venzke-Caprese* (Fn. 12), 779. Der nicht verabschiedete Entwurf eines Arbeitnehmerdatenschutzgesetzes schlug in § 32 Abs. 6 Satz 2 BDSG eine Sonderregelung vor: Er gestand dem Arbeitnehmer gegen die Datenerhebung des Arbeitgebers in sozialen Netzwerken (mit Ausnahme von beruflichen Netzwerken) ein überwiegendes Schutzinteresse zu; BT-Drucks. 17/4230, S. 6 u. 16. Dazu auch *Ernst*, NJOZ 2011, 953 (954 ff.); *Klas*, Grenzen der Erhebung und Speicherung allgemein zugänglicher Daten, 2012, S. 59 ff.

[96] BT-Drucks. 7/1027, S. 22; *Venzke-Caprese* (Fn. 12), 777.

[97] Dazu auch bereits oben unter II. 1., S. 17.

[98] Siehe etwa stellvertretend § 12 Abs. 1 Satz 1, § 13 Abs. 1, Abs. 2 Satz 1 lit. f NRWDSG.

[99] § 1 Abs. 7 BremDSG; § 2 Abs. 6 HmbDSG; § 3 Abs. 4 HDSG und § 2 Abs. 5 Satz 1 RhPfLDSG („Dieses Gesetz gilt nicht für…"). In Rheinland-Pfalz gilt jene Ausnahme vom Anwendungsbereich aber nicht, sofern die allgemein zugänglichen Daten gesondert gespeichert und weiterverarbeitet werden (§ 2 Abs. 5 Satz 2 RhPfLDSG), insbesondere bei der Herauslösung aus dem ursprünglichen Verwendungszusammenhang oder dem Zusammenführen von Einzelinformationen aus unterschiedlichen, allgemein zugänglichen Quellen. Genau dabei handelt es sich aber um

Anwendungsbereich ihrer Datenschutzgesetze aus. Diese Sonderregelungen zielen nach ihrer normativen Idee auf den besonderen Schutz der Informationsfreiheit[100] - ohne dass öffentliche Stellen diesen Schutz jedoch grundrechtlich genießen. Nimmt man die Vorschriften beim Wort, ist in den vier Ländern jegliche Form der Verarbeitung und Nutzung allgemein zugänglicher Quellen durch öffentliche Stellen zulässig. Mit den Vorgaben der Art. 6 und 7 der Datenschutzrichtlinie 95/46/EG ist ein solches Verständnis allerdings nicht vereinbar. Bereichsausnahmen für die Verarbeitung personenbezogener Daten lässt die Datenschutzrichtlinie nämlich – ähnlich wie in Zukunft Art. 2 Abs. 2 DSGVO – nur für solche Verarbeitungen zu, die ausschließlich zu persönlichen oder familiären Tätigkeiten vorgenommen werden oder nicht in den Anwendungsbereich des Unionsrechts fallen (Art. 3 Abs. 2 RL 95/46/EG).[101] Die behördliche Auswertung in sozialen Netzwerken allgemein zugänglicher Quellen erfüllt keinen dieser Ausnahmetatbestände.[102] In unionsrechtskonformer Auslegung erstreckt sich die Privilegierung der Nutzung allgemein zugänglicher Quellen daher jedenfalls nicht auf die Auswertung und Zusammenführung im Wege eines Social Media Monitorings. Das deutet nicht nur die normative Einschränkung „solange sie in allgemein zugänglichen Quellen gespeichert sind“ vorsichtig an (§ 2 Abs. 5 Satz 2 RhPfLDSG). Vor allem halten die Länder für Verarbeitungen öffentlicher Stellen, die Daten aus allgemein zugänglichen Quellen entnehmen, eine zusätzliche Verarbeitungsgrundlage vor (vgl. z. B. § 12 Abs. 2 Nr. 6 BremDSG). Ihrer bedarf es denklogisch nur dann, wenn nicht bereits die allgemeine Bereichsausnahme greift. Social Media Monitoring öffentlicher Stellen unterliegt mithin auch in Bremen, Hamburg, Hessen und Rheinland-Pfalz den allgemeinen Rechtfertigungsanforderungen, welche die Datenschutzgesetze formulieren.

a) Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgabe – § 13 Abs. 1, § 14 Abs. 1 Satz 1 BDSG

Der Grundrechts- und Gesetzesbindung öffentlicher Stellen entspricht es, ihr Monitoring nicht für jeden denkbaren Zweck zuzulassen, sondern es immer an eine öffentliche Aufgabe und die eigene Zuständigkeit der datenverarbeitenden Behörde rückzubinden. So verfügen es § 13 Abs. 1 und § 14

typische Anwendungsbereiche des Social Media Monitorings. Es greifen dann die Rechtfertigungstatbestände des § 12 Abs. 4 Satz 1 Nr. 9 und Satz 2 sowie § 13 Abs. 2 Nr. 1 RhPfLDSG.

[100] Vgl. RhPfLT-Drucks. 12/3824, S. 33 f.; *Globig/Schuber/Hartig et al.*, in: dies. (Hrsg.), RhPfLDSG, 2009, § 2, 5.1.; *Schild/Ronellenfitsch/Arlt et al.*, in: dies. (Hrsg.), HDSG, 2016, § 3, 5.1.

[101] Weiter geht (pro futuro) prima facie Art. 85 Abs. 1 DSGVO: Er gesteht den Mitgliedstaaten nach seinem Wortlaut den Regelungsauftrag und das Recht zu, den Persönlichkeitsschutz und die Informationsfreiheit durch eigene Regelungen zum Ausgleich zu bringen. Vgl. dazu auch unten IV. 2., S. 45.

[102] So bereits für den Ausnahmetatbestand persönlicher bzw. familiärer Tätigkeiten EuGH, Urteil vom 6.11.2003 – Lindqvist –, ECLI:EU:C:2003:596, Rdnr. 46 f.

Abs. 1 BDSG bzw. zahlreiche Landesdatenschutzgesetze[103] unmissverständlich. Damit schränken sie den Handlungsrahmen für ein Social Media Monitoring öffentlicher Stellen nicht unerheblich ein.[104]

b) Erforderlichkeit des Monitorings zur Aufgabenerfüllung

Die bloße *Nützlichkeit* eines Social Media Monitorings für die Aufgabenerfüllung genügt bei öffentlichen Stellen anders als bei Privaten nicht. Die Datenerhebung und -verarbeitung muss vielmehr dafür *erforderlich* sein (§ 13 Abs. 1 und § 14 Abs. 1 BDSG).[105] Das ist sie nur, wenn die im Zuständigkeitsbereich der verantwortlichen Stelle liegende Aufgabe ohne die Datenverwertung nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllbar wäre.[106] Mit diesem strengen Maßstab [107] wollte der Gesetzgeber erklärtermaßen „ein unnötiges Eindringen in den Persönlichkeitsbereich" der Bürger verhindern und „dem Zusammentragen aller Informationen über eine Person zu einem geschlossenen Persönlichkeitsbild eine Grenze" setzen – sowohl in der zeitlichen als auch in der inhaltlichen Erstreckung der Datenvorhaltung.[108] Lässt sich die Aufgabe ohne das Monitoring gleich wirksam wahrnehmen, ist im Zweifel ein Verzicht geboten. Unzulässig ist es daher etwa, wenn eine Baubehörde via Social Media Monitoring allgemein Informationen über die politischen Einstellungen bestimmter Bürger einsammelt. Kommunale Online-Partizipationsportale auf die Repräsentativität und gruppenspezifische Ausrichtung der User-Beiträge (Alter, Geschlecht, Wohnort, unmittelbar versus mittelbar Betroffene etc.) zu untersuchen, kann demgegenüber zulässig sein.[109] Denn ohne diese Informationen lässt sich der Aussagegehalt der Beiträge regelmäßig nicht sachgerecht oder nur eingeschränkt beurteilen.

aa) Vorrang der Direkterhebung (§ 4 Abs. 2 BDSG)

Nicht erforderlich ist das Monitoring grundsätzlich, wenn die Behörde die Daten auch unmittelbar bei dem Betroffenen erheben könnte. Das ist Ausdruck des Direkterhebungsgrundsatzes, den § 4 Abs. 2 Satz 1 BDSG etabliert.[110]

---

[103] Siehe insbesondere § 12 Abs. 1 Satz 1 und § 13 Abs. 1 Satz 1 NRWDSG.
[104] Zum künftigen Regelungsregime der DSGVO siehe unten IV. 1., S. 46
[105] Ebenso für das Landesrecht beispielsweise § 12 Abs. 1 Satz 1 NRWDSG und § 13 Abs. 1 Satz 1 NRWDSG.
[106] *Dammann*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 14, Rdnr. 15; *Roggenkamp*, in: Plath (Hrsg.), BDSG, 2013, § 14 BDSG, Rdnr. 3.
[107] *Dammann* (Fn. 104), § 14, Rdnr. 12 m. w. N.
[108] Begründung zu § 6, BT-Drucks. 7/1027, S. 24. Die noch im Regierungsentwurf vorgesehene, sich an § 28 Abs. 1 Nr. 1 BDSG a. F. („im Rahmen der Zweckbestimmung eines Vertragsverhältnisses") anlehnende Formulierung „im Rahmen" hat der Gesetzgeber aus eben diesem Grunde nicht übernommen.
[109] Dazu *Martini/Fritzsche* (Fn. 40), S. 92.
[110] Der Direkterhebungsgrundsatz gilt auch im Landesrecht, siehe exempli causa § 12 Abs. 1 Satz 3 NRWDSG. Die DSGVO kennt einen Direkterhebungsgrundsatz i. S. d. BDSG nicht. Dazu unten IV. 3. a., S. 47.

(1) Gesetzliche Erlaubnis im Sinne des § 4 Abs. 2 Satz 2 Nr. 1 Alt. 1 BDSG?

Regelungen, welche die Verarbeitung allgemein zugänglicher Daten bzw. Quellen ermöglichen, lassen sich zwar gerade als Ausnahme vom Direkterhebungsgrundsatz i. S. d. § 4 Abs. 2 Satz 2 Nr. 1 Alt. 1 BDSG verstehen.[111] Auf die Tatbestände, die *privaten Stellen* ein Auswertungs- und Nutzungsprivileg für eine Datenerhebung aus allgemein zugänglichen Quellen zugestehen (etwa § 28 Abs. 1 Satz 1 Nr. 3 BDSG), trifft das uneingeschränkt zu; sie sehen eine Erhebung ohne Mitwirkung des Betroffenen ausdrücklich vor.

Gleiches gilt aber *nicht* für die – auf den ersten Blick ähnliche – Regelung des § 14 Abs. 2 Nr. 5 BDSG[112] *für öffentliche Stellen.* Sie gestattet zwar das Speichern, Verändern oder Nutzen allgemein zugänglicher Daten. Sie formuliert aber (anders als dies § 13 Abs. 2 Nr. 4 BDSG für Daten, die der Betroffene offenkundig öffentlich gemacht hat, sowie manche Landesdatenschutzgesetze ausdrücklich für ihre öffentlichen Stellen bei der Entnahme von Daten aus allgemein zugänglichen Quellen tun[113]) keine gesetzliche Ausnahme von dem Gebot der Direkterhebung i. S. d. § 4 Abs. 2 Satz 2 Nr. 1 Alt. 2 BDSG. Vielmehr befreit sie lediglich von der *Zweckbindung* bei diesen Verarbeitungsvorgängen. Sie setzt voraus, dass die Daten bereits anderweit erhoben worden sind. Da § 14 (im Unterschied zu § 13 BDSG) nicht die Erhebung regelt, kann er auch keine Ausnahme vom Direkterhebungsgrundsatz etablieren.[114] Bei der ersten Datenerhebung gilt für öffentliche

---

[111] In diesem Sinne (jedenfalls zu den Vorschriften der §§ 28 ff. BDSG) *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 4, Rdnr. 24; *Solmecke* (Fn. 93), Rdnr. 44; *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl., 2013, § 4 BDSG, Rdnr. 65; *Venzke-Caprese* (Fn. 12), 778. Im Ergebnis ebenso *Kramer*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 4 BDSG, Rdnr. 20; anders bzw. irrig *Jung*, PinG 3 (2015), 170 (173).

[112] Einige Bundesländer halten inhaltlich gleichlaufende Parallelnormen vor; siehe § 13 Abs. 2 Satz 1 lit. f BbgDSG; § 12 Abs. 2 Satz 1 Nr. 6 BremDSG; § 13 Abs. 2 Satz 1 Nr. 7 HmbDSG; § 10 Abs. 3 Satz 1 Nr. 5 i. V. mit § 11 Abs. 2 DSG M-V; § 10 Abs. 2 Satz 1 Nr. 2 i. V. mit § 9 Abs. 1 Satz 3 Nr. 5 NdsDSG; § 13 Abs. 2 Satz 1 lit. f NRWDSG; § 13 Abs. 2 Satz 1 lit. f SaarlDSG und § 10 Abs. 2 Nr. 5 DSG LSA.

Andere Bundesländer kennen das Zweckänderungsprivileg zwar auch, schränken es aber stärker ein als der Bund. Während das BDSG das Privileg erst entfallen lässt, wenn schutzwürdige Interessen des Betroffenen *offensichtlich* überwiegen, reicht in diesen Ländern, dass schutzwürdige Interessen des Betroffenen entgegenstehen bzw. überwiegen, ohne dass dies offensichtlich sein muss (§ 15 Abs. 2 Nr. 7 BWLDSG; § 11 Abs. 2 Nr. 1 i. V. mit § 6 Abs. 1 Satz 2 BlnDSG; § 13 Abs. 2 Nr. 1 i. V. mit § 12 Abs. 4 Satz 1 Nr. 9, Satz 2 RhPfLDSG; § 13 Abs. 2 Nr. 2 SächsDSG; § 20 Abs. 2 Nr. 5 ThürDSG). Strenger demgegenüber § 13 Abs. 2 i. V. mit § 12 Abs. 2 und 3 HDSG; speziell für in allgemein zugänglichen Quellen gespeicherte Daten sieht das HDSG in § 3 Abs. 4 jedoch eine Bereichsausnahme vor (siehe dazu bereits Fußn. 99). Bayern lässt die Nutzung aus öffentlichen Quellen erhobener Daten hingegen grundsätzlich unbeschränkt zu (Art. 17 Abs. 2 Nr. 8 BayDSG).

[113] § 13 Abs. 2 BWLDSG; Art. 16 Abs. 2 Satz 1 BayDSG; § 9 Abs. 1 Satz 3 lit. e NdsDSG; § 13 Abs. 4 Nr. 9 RhPfLDSG; § 12 Abs. 3 i. V. mit § 13 Abs. 2 Satz 1 lit. f SaarlDSG; § 12 Abs. 2 und 3 SächsDSG.

[114] Denkbar ist jedoch, dass der Auswertung allgemein zugänglicher Quellen im Wege eines Social Media Monitorings keine Erhebung vorausgeht (vgl. § 14 Abs. 1 Satz 2 BDSG). Dieser Gedanke scheint jedenfalls den Datenschutzgesetzen Nordrhein-Westfalens und des Saarlandes zugrunde zu liegen. Sie privilegieren zwar die Zweckänderung bei der Weiterverarbeitung personenbezogener Daten bei der Entnahme aus allgemein zugänglichen Quellen, schließen aber eine (ihr sachlogisch vorangehende) Erhebung der öffentlichen Stelle bei Dritten explizit aus (besonders deutlich bringen das § 12 Abs. 1 Satz 3 i. V. mit § 13 Abs. 2 lit. f NRWDSG e contrario und § 12 Abs. 4 Satz 1 i. V. mit § 13 Abs. 2 Satz 1 lit. f

Stellen vielmehr das Erforderlichkeitsprinzip (§ 13 Abs. 1 BDSG) und mit ihm – solange das Gesetz nicht ausdrücklich, wie z. B. für nicht-öffentliche Stellen in § 28 Abs. 1 Satz 1 Nr. 3 BDSG, die Erhebung aus allgemein zugänglichen Quellen gestattet – der Direkterhebungsgrundsatz (§ 4 Abs. 2 Satz 1 BDSG).

(2) Natur der Verwaltungsaufgabe und unverhältnismäßiger Aufwand als Ausnahme vom Direkterhebungsgrundsatz (§ 4 Abs. 2 Nr. 2 BDSG)

Dispensiert § 14 Abs. 2 Nr. 5 BDSG also nicht von dem Direkterhebungsgrundsatz, dürfen öffentliche Stellen Daten aus allgemein zugänglichen Quellen nur dann erheben, wenn die öffentliche Aufgabe ihrer Art nach[115] verlangt, dass die Erhebung bei anderen Personen oder Stellen erfolgt (§ 4 Abs. 2 Satz 2 Nr. 2 lit. a BDSG[116]) oder die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordert (§ 4 Abs. 2 Satz 2 Nr. 2 lit. b BDSG[117]).[118] Letzteres trifft regelmäßig zu, wenn die Aufgabenerfüllung die Analyse eines breiten Querschnitts gerade in den sozialen Medien zu findender Informationen erfordert, also in besonderer Weise auf die technischen Möglichkeiten eines Social Media Monitorings angewiesen ist, z. B. bei einer allgemeinen Tonalitätsanalyse der Bundesregierung zu aktuellen politischen Themen.

Die Unverhältnismäßigkeit des Aufwands alleine genügt aber nicht. Nach der Wertung des Gesetzgebers dürfen zusätzlich auch keine Anhaltspunkte dafür bestehen, dass die mittelbare Erhebung „überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt“ (§ 4 Abs. 2

SaarlDSG zum Ausdruck; ähnlich in der Sache § 10 Abs. 4 BlnDSG; § 10 Abs. 3 i. V. mit § 12 Abs. 2 Nr. 6 BremDSG [anders demgegenüber Art. 16 Abs. 2 Satz 1 BayDSG; § 12 Abs. 3 i. V. mit § 13 Abs. 2 Satz 1 lit. f BbgDSG; § 12 Abs. 4 Satz 1 Nr. 9 RhPfLDSG; § 11 Abs. 2 SchlHLDSG]). In die Richtung fehlender Erhebung deutet auch die variierende gesetzliche Terminologie: In diesen Fällen spricht das Gesetz nicht davon, dass Daten aus allgemein zugänglichen Quellen „erhoben“, sondern „entnommen“ werden (so z. B. § 10 Abs. 3 Satz 1 Nr. 5 DSG M-V; § 9 Abs. 2 Satz 3 lit. e NdsDSG). Gleichzeitig liegen die Anforderungen, die das BDSG begrifflich an eine Erhebung stellt, nicht hoch. Es genügt die willentliche Kenntnisnahme von Daten, welche dem Verarbeiter nicht allein zufällig, etwa aufgrund des Umstandes, dass er eine Kommunikationseinrichtung, z. B. ein Postfach, vorhält, zuwachsen; *Dammann*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 3, Rdnr. 104; *Martini/Fritzsche* (Fn. 8), S. 7. Ein Social Media Monitoring setzt die Beschaffung von Informationen (seien sie auch allgemein zugänglich) konzeptionell notwendig voraus. Vgl. dazu auch oben I. 4., S. 9.

Die Zulässigkeit einer Erhebung knüpft § 13 Abs. 1 BDSG daran, dass sie zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. § 13 Abs. 1a BDSG scheint zwar auf den ersten Blick den öffentlichen Stellen eine Hinweispflicht gegenüber der externen Erhebungsquelle aufzuerlegen. Die Vorschrift geht jedoch implizit von einer nicht allgemeinen Zugänglichkeit der Quelle aus („zur Auskunft verpflichtet“) und ist deshalb nicht einschlägig.

[115] Denkbar ist das z. B. vor einer öffentlichen Ehrung sowie dann, wenn die Aufgabe darin besteht, Angaben des Betroffenen auf ihre Richtigkeit zu überprüfen.

[116] Für die Landesgesetze etwa § 13 Abs. 4 Nr. 2 BWLDSG; § 9 Abs. 2 Satz 2 Nr. 2 lit. a DSG LSA; § 19 Abs. 2 Satz 2 Nr. 2 ThürDSG.

[117] Ebenso § 13 Abs. 4 Nr. 1 i. V. mit § 15 Abs. 2 Nr. 6 BWLDSG; § 9 Abs. 2 Satz 2 Nr. 2 lit. b DSG LSA; § 13 Abs. 1 Satz 2 i. V. mit Abs. 3 Nr. 4 SchlHLDSG; § 19 Abs. 2 Satz 2 Nr. 3 ThürDSG.

[118] Den normativen Katalog der Ausnahmen vom Direkterhebungsgrundsatz gestalten einige Länder offener als das BDSG, so etwa § 12 Abs. 3 BbgDSG; § 12 Satz 3 HmbDSG; § 9 Abs. 1 Satz 3 Nr. 5 NdsDSG; § 12 Abs. 1 Satz 3 NRWDSG; § 12 Abs. 4 RhPfLDSG; § 12 Abs. 4 SächsDSG.

Satz 2 BDSG a. E. [119]). Diese Einschränkung trägt dem besonderen Schutzbedürfnis des informationellen Selbstbestimmungsrechts Rechnung.[120]

Nicht schutzwürdig ist der Betroffene, wenn er Informationen *selbst* für *jedermann* öffentlich kundgetan hat. Das gilt nach der normativen Wertentscheidung des § 14 Abs. 5 Satz 1 Nr. 1 i. V. mit § 13 Abs. 2 Nr. 4 BDSG[121] sogar bei sensiblen Gesundheitsdaten oder einer Parteizugehörigkeit.[122] Wer Informationen selbst öffentlich gemacht hat, darf für deren Verarbeitung durch Dritte nicht den Schutz der Rechtsordnung reklamieren. Denn jeder hat nach dem Verantwortungsprinzip die Konsequenzen seines autonomen Verhaltens zu tragen.[123]

Das setzt aber sachlogisch die willentliche Entäußerung der Daten durch die betreffende Person in einer Weise voraus,[124] die einen Verbreitungswillen nach außen manifestiert.[125] Es darf also keine berechtigten Zweifel daran geben, dass der Betroffene selbst und nicht ein Dritter die Daten öffentlich gemacht hat. Zudem muss sich die Veröffentlichung bewusst auch an die gesamte Internetöffentlichkeit, nicht nur an Teil-Öffentlichkeiten (etwa eine Netzwerk-Community) richten. Der Betroffene darf insbesondere keine – z. B. durch robots.txt[126] bekundeten – Einwände gegen eine Erfassung durch jedermann, auch öffentliche Stellen, ohne Rücksicht auf deren Identität zu erkennen gegeben haben.[127]

---

[119] Siehe auch ähnlich § 13 Abs. 4 Nr. 2 BWLDSG; § 12 Abs. 4 Satz 2 RhPfLDSG; § 9 Abs. 2 Satz 2 Nr. 2 DSG LSA und § 19 Abs. 2 Satz 3 ThürDSG.

[120] Vgl. dazu *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl., 2015, § 4 BDSG, Rdnr. 6.

[121] Die Vorschrift geht zurück auf Art. 8 Abs. 2 lit. e der Datenschutzrichtlinie 95/46/EG. Vgl. dazu auch *Eßer*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 13 BDSG, Rdnr. 31; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 13, Rdnr. 18; *Stender-Vorwachs*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 13 BDSG, Rdnr. 31. Vergleichbare Regelungen finden sich auf landesrechtlicher Ebene in Art. 15 Abs. 7 Nr. 4 BayDSG; § 3 Abs. 2 Nr. 4 BremDSG; § 5 Abs. 1 Satz 2 Nr. 3 HmbDSG; § 4 Abs. 3 Satz 2 Nr. 3 NRWDSG; § 13 Abs. 3 i. V. mit § 12 Abs. 5 Nr. 3 RhPfLDSG; § 4 Abs. 2 Nr. 3 SaarlDSG; § 4 Abs. 2 Nr. 4 SächsDSG; § 26 Abs. 1 Nr. 4 DSG LSA; § 11 Abs. 3 Nr. 5 SchlHLDSG und § 4 Abs. 5 Nr. 4 ThürDSG.

[122] Vgl. auch § 28 Abs. 6 Nr. 2 BDSG im Falle der Erhebung und Speicherung privater Stellen für eigene Geschäftszwecke. Bei der geschäftsmäßigen Erhebung und Speicherung für Zwecke der Markt- oder Meinungsforschung dürfen besondere Arten personenbezogener Daten nur für ein bestimmtes Forschungsvorhaben erhoben, verarbeitet oder genutzt werden (§ 30a Abs. 1 Satz 2 BDSG). Wenn die verantwortliche private Stelle die Richtigkeit der sensiblen Daten nicht beweisen kann, sind sie zu löschen; das gilt auch für strafbare Handlungen und Ordnungswidrigkeiten (§ 35 Abs. 2 Nr. 2 BDSG).

[123] *Nettesheim*, VVDStRL 70 (2011), 7 (41). Hierzu auch oben II. 1., S. 17.

[124] *Stender-Vorwachs* (Fn. 119), § 13 BDSG, Rdnr. 31. Ähnlich auch *Gola/Klug/Körffer* (Fn. 119), § 13, Rdnr. 38.

[125] *Wedde*, in: Däubler/Klebe/Wedde et al. (Hrsg.), BDSG, 5. Aufl., 2016, § 28, Rdnr. 171; *ULD Schleswig-Holstein*, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, 2014, S. 127.

[126] Die Datei „Robots Exclusion Standard Protokoll“ steuert das Auswertungsverhalten von Suchmaschinen: Sie weist diese an, bestimmte in eine Website eingespeiste Informationen von der Analyse auszunehmen und damit ihre Auffindbarkeit zu erschweren.

[127] *Eßer* (Fn. 119), § 13 BDSG, Rdnr. 31 unter Verweis auf *Wedde*, in: Däubler/Klebe/Wedde et al. (Hrsg.), BDSG, 5. Aufl., 2016, § 13, Rdnr. 31 f.; *Sokol/Scholz*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 13, Rdnr. 38; a. A. *Roggenkamp*, in: Plath (Hrsg.), BDSG, 2013, § 13 BDSG, Rdnr. 19.

Hat der Betroffene die Informationen *nicht selbst offenbart,* genießt die Autonomie über die eigenen Daten im Verhältnis zu einem Auswertungsinteresse Dritter im Zweifel den Vorrang. Gerade bei Informationen, die aus der Verknüpfung verschiedener allgemein zugänglicher Daten stammen, welche der Betroffene nicht unbedingt selbst kundgetan hat, erhöht sich die Intransparenz für den Betroffenen sprunghaft. Für ihn ist dann nicht mehr erkennbar, welche Daten sich Dritte über ihn verschaffen und wie sie diese verarbeiten.

bb) Zwischenergebnis

Die Zusammenführung verfügbarer Informationen zu einer übergreifenden Datenanalyse im Wege eines Social Media Monitorings statt einer individuellen Abfrage beim Betroffenen gestattet das Datenschutzrecht nicht ohne Weiteres. Vielmehr zeichnet es die Direkterhebung als normativen Regelfall vor. Nur wenn sich diese als unverhältnismäßig oder nach der Art der Aufgabe untunlich erweist, ist das Monitoring erforderlich i. S. d. § 13 Abs. 1 und § 14 Abs. 1 BDSG. Dem Social Media Monitoring öffentlicher Stellen setzt das Gesetz damit im Ergebnis enge Grenzen. So hat eine Behörde grundsätzlich durch direkte Befragung und nicht durch Social Media Monitoring zu erforschen, ob ein Empfänger von Sozialleistungen zusätzliche Einnahmen hat (§ 67a Abs. 2 Satz 2 Nr. 1 SGB X).

Für Daten, die der Betroffene offenkundig selbst für jedermann öffentlich gemacht hat, gilt das jedoch nicht. Der Gesetzgeber lässt deren Erhebung und Verwertung auch bei besonderen Arten personenbezogener Daten unmittelbar aus der öffentlich zugänglichen Quelle zu (§ 13 Abs. 2 Nr. 4 BDSG). Öffentliche Stellen dürfen diese daher grundsätzlich – im Rahmen des Erforderlichen – als Teil eines Social Media Monitorings erfassen.

c) Befreiung von der Zweckbindung bei der Nutzung allgemein zugänglicher Daten

Obgleich sich öffentliche Stellen anders als Private nicht auf die Informationsfreiheit berufen können, gesteht der einfache Gesetzgeber ihrem Zugriff auf allgemein zugängliche Daten gleichwohl eine Privilegierung zu: Sie dürfen allgemein zugängliche Daten (aa) ohne Rücksicht auf den Zweck auswerten, zu dem sie veröffentlicht[128] worden sind, soweit nicht schutzwürdige Interesse des Betroffenen offensichtlich überwiegen (bb). So bestimmen es § 14 Abs. 2 Nr. 5 BDSG bzw. die

[128] § 14 Abs. 1 Satz 1 BDSG nimmt in seinem Wortlaut zwar Bezug auf die behördliche Datenerhebung, nicht aber auf die Veröffentlichung der Daten durch Betroffene. Insbesondere entfällt im Falle des Social Media Monitorings nicht die Daten*erhebung* (§ 14 Abs. 1 Satz 2 BDSG), sondern es findet eine zielgerichtete Beschaffung von Daten statt (vgl. auch Fußn. 114). Seinem Sinn nach rekurriert das Gesetz aber hinsichtlich der Zweckbindung auf den Veröffentlichungskontext, den der Betroffene seiner allgemeinen Zugänglichmachung der Information zugeschrieben hat. Das deutet § 14 Abs. 2 Nr. 5 BDSG auch mit der Wendung „veröffentlichen dürfte“ vorsichtig an. Insoweit ist der Wortlaut in Anlehnung an § 14 Abs. 1 Satz 2 BSDG teleologisch zu reduzieren.

entsprechenden Parallelnormen der Landesdatenschutzgesetze [129]. Der Einzelne kann der öffentlichen Stelle die ursprüngliche Zweckbindung der Daten dann nicht entgegenhalten.

aa) Allgemein zugängliche Daten

Nicht jedes Datum, das im Internet verfügbar ist, ist allgemein zugänglich. Auf Daten sozialer Netzwerke trifft das vielmehr – ähnlich wie nach § 19a UrhG [130] – nur dann zu, wenn ihre Abrufbarkeit nicht auf einen bestimmten Nutzerkreis, also eine individuell bestimmbare Personengruppe, beschränkt ist.[131]

Ob Informationen geeignet und bestimmt sind, der Allgemeinheit zur Information zu dienen (und damit die begrifflichen Anforderungen der Informationsfreiheit i. S. d. Art. 5 Abs. 1 Satz 1 Var. 2 GG erfüllen), [132] ist entgegen teilweise vertretener Auffassung [133] für den Begriff der allgemein zugänglichen Quelle im BDSG grundsätzlich nicht maßgeblich. Den Regelungen des § 10 Abs. 5 Satz 2, § 14 Abs. 2 Nr. 5 [134] und § 28 Abs. 1 Satz 1 Nr. 3 BDSG kommt es ausweislich des Gesetzeswortlauts nicht darauf an, ob die Informationen zur Wahrnehmung durch jedermann *bestimmt* sind. Entscheidend ist vielmehr, ob die Internetöffentlichkeit von der Kenntnisnahme der Inhalte *tatsächlich* ausgeschlossen ist oder ob jeder die Informationen ungehindert abrufen *kann*. Bei öffentlich abrufbaren Informationen eines Facebook-Profils oder Twitter-Accounts ist diese Voraussetzungen jedenfalls erfüllt: Jeder kann sich durch Direktzugriff oder über Suchmaschinen ein Bild von ihnen machen.

---

[129] Siehe dazu Fußn. 112.

[130] Den Begriff der allgemein zugänglichen Quelle bzw. der öffentlichen Zugänglichmachung kennt das Gesetz auch in verschiedenen anderen normativen Kontexten. § 19a UrhG verwendet den Begriff der öffentlichen Zugänglichmachung (in wörtlicher Übereinstimmung mit der Urheberrechtsrichtlinie 2001/29/EG) im Sinne einer Zugänglichmachung für die Mitglieder der Öffentlichkeit unabhängig von Ort und Zeit, also für alle, die nicht mit dem Verwerter des Werkes durch persönliche Beziehungen verbunden sind.

[131] *Klas* (Fn. 93), S. 41 ff.; *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl., 2013, § 28 BDSG, Rdnr. 82 f.; *Venzke-Caprese* (Fn. 12), 776 mit Verweis u. a. auf *Ernst* (Fn. 93), 955; siehe auch *Bergmann/Möhrle/Herb*, in: dies. (Hrsg.), DatenschutzR, 48. Erg.-Lfg., Feb. 2015, § 28 BDSG, Rdnr. 263; *Kramer*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 28 BDSG, Rdnr. 20; *ULD Schleswig-Holstein* (Fn. 123), S. 127.

[132] BVerfG, Beschluss vom 3.10.1969, BVerfGE 27, 71 (83).

[133] *Plath*, in: ders. (Hrsg.), BDSG, 2013, § 28 BDSG, Rdnr. 76; *Schreiber* (Fn. 12), 35; *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl., 2015, § 28 BDSG, Rdnr. 7; *Stender-Vorwachs* (Fn. 119), § 13 BDSG, Rdnr. 38; *Venzke-Caprese* (Fn. 12), 776; *Wedde* (Fn. 123), § 28, Rdnr. 58.

[134] Diese für öffentliche Stellen geltende Vorschrift steht überdies nicht im Dienste des verfassungsrechtlichen Schutzes der Informationsfreiheit. Dazu bereits oben III. 2., S. 25.

(1) Allgemeine Zugänglichkeit trotz Anmeldeerfordernis

Viele soziale Netzwerke oder Internetforen schalten einem Zugang zu ihren Informationen ein Anmeldeerfordernis vor, das den Zugang zur Information erschwert.[135] Nach dem Willen des Gesetzgebers schließt das ihre allgemeine Zugänglichkeit – und damit den grundsätzlichen gesetzlichen Vorrang des Auswertungsinteresses – jedoch nicht von vorneherein aus.[136] So will es die Legaldefinition des § 10 Abs. 5 Satz 2 BDSG[137]: Sie abstrahiert den Begriff der allgemeinen Zugänglichkeit davon, ob eine Anmeldung erforderlich ist oder nicht („sei es ohne oder nach vorheriger Anmeldung").[138]

Nach dem Sinn der Vorschrift kann das aber nur so lange gelten, wie eine Anmeldung jedermann offen steht. Erkennbare Zugangsbeschränkungen sind zu respektieren. In besonderer Weise gilt dies für Informationen, die etwa nur Facebook-„Freunden", einer geschlossenen Gruppe oder individuell eingeladenen Diskussionsteilnehmern vorbehalten sind.[139] Dritten ist der Zugriff auf netzwerkinterne Daten mangels allgemeiner Zugänglichkeit dann versperrt. Nicht alle nach erfolgter Authentifizierung sichtbaren Daten sind deshalb auch allgemein zugänglich.

Auch ausdrückliche Beschränkungen des Diensteanbieters, die er in seinen Nutzungsbestimmungen vorsieht, limitieren die allgemeine Zugänglichkeit netzwerkinterner Daten – etwa wenn ein soziales Netzwerk die Anmeldung natürlichen Personen mit Klarnamenprofil vorbehält.[140] Denn allgemein zugänglich ist nur das, was jedermann – wenn auch nach rechtmäßiger Überwindung von Zulassungshindernissen – zur Kenntnis nehmen kann. Der rechtswidrig verschaffte Zugang – etwa durch die Kreation eines Pseudonyms, mit dessen Hilfe eine Behörde unter Verstoß gegen die Nutzungsregeln die Identität einer natürlichen Person suggeriert – genießt nicht das datenschutzrechtliche Privileg, das allgemein zugänglichen Daten zukommt. Daten, die sich hinter erkennbaren, nicht von jedermann – insbesondere auch staatlichen Behörden – in rechtlich zulässiger Weise überwindbaren Zugangsbeschränkungen verbergen, sind dem Social Media Monitoring deshalb von vorneherein entzogen.

---

[135] *Wolff*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 28 BDSG, Rdnr. 83.

[136] A. A. wohl *Brus/Schwab*, Medizinische Einsatzmöglichkeiten von Big Data oder Big Data im Gesundheitswesen - am Datenschutz erkrankt?, in: Taeger (Hrsg.), Big Data & Co, 2014, S. 171 (178 f.). Wie hier aber beispielsweise (wenn auch ohne Rekurs auf § 10 Abs. 5 Satz 2 BDSG) *Jandt/Roßnagel*, ZD 2011, 160 (165).

[137] Mit Ausnahme des § 2 Abs. 1 Satz 3 SächsDSG definieren die Landesdatenschutzgesetze den Begriff der allgemein zugänglichen Daten nicht ausdrücklich, geben aber kein anderes Begriffsverständnis als das BDSG zu erkennen.

[138] *Venzke-Caprese* (Fn. 12), 776; das übersieht *Schreiber* (Fn. 12), 35.

[139] Dazu *Graf*, in: ders. (Hrsg.), BeckOK StPO, 25. Ed., Stand: 2016, § 100a StPO, Rdnr. 32i; *Klas* (Fn. 93), S. 42.

[140] Ebenso für den Parallelfall des § 19a UrhG BGH, Urteil vom 29.4.2010, GRUR 2011, 56 (59, Rdnr. 30). Danach differenzierend, ob die Plattform die Nutzungsbeschränkungen (etwa auf Volljährigkeit oder Angabe des Klarnamens) auch tatsächlich vor der Anmeldung überprüft *Venzke-Caprese* (Fn. 12), 776 mit Fußn. 11.

(2) Unautorisierte Veröffentlichung durch Dritte und rechtswidrig erhobene Daten

Nicht alle personenbezogenen Daten, die allgemein zugänglich sind, wollte der Betroffene dem Internetpublikum auch unbedingt allgemein zugänglich machen. Das gilt etwa für Informationen, die Personen als „informationelle Gegenbilder“[141] über Dritte ins Netz stellen.[142] Man denke etwa an das Nacktfoto, das der ehemalige Partner als Rache im Netz hochlädt, ein von einem notorischen Fan angelegtes Fake-Profil eines Prominenten oder die Veröffentlichung unautorisierter Gesprächsmitschnitte.

Knüpfte das Gesetz die Zulässigkeit der Verarbeitung an den Veröffentlichungswillen, müsste also der Betroffene die Inhalte jeweils auch allgemein zugänglich machen *wollen*, erwüchse daraus ein wirksamer Missbrauchsschutz. Einen solchen sieht das Gesetz aber – entgegen vielfach vertretener Auffassung[143] – in dieser Gestalt nicht vor: Es hebt auf die objektive Zugänglichkeit ab („nutzen kann“) – nicht auf Motivationen. Insbesondere differenziert es in seiner Terminologie bewusst feinsäuberlich zwischen offenkundig durch den Betroffenen verlautbarten (§ 13 Abs. 2 Nr. 4 BDSG)[144] und allgemein zugänglichen Informationen (§ 14 Abs. 2 Nr. 5 BDSG). Auch ein Widerspruch Betroffener, der die Verbreitung oder Zugänglichmachung für jedermann unterbinden will, schließt als solcher die allgemeine Zugänglichkeit noch nicht aus.[145]

α) Dogmatischer Berücksichtigungsort

Allgemein zugänglich i. S. d. § 10 Abs. 5 Satz 2 BDSG sind im Grundsatz sogar solche Daten, die rechtswidrig, insbesondere unter Verstoß gegen deutsches Datenschutzrecht, erhoben worden sind und dennoch den Weg an die Öffentlichkeit gefunden haben. Der Staat, der diese Daten verarbeitet, erntet dann gleichsam von den Früchten des verbotenen Baumes. Darf er Daten, deren Erhebung er einerseits für rechtswidrig erklärt, andererseits rechtmäßig verwerten und damit bestehendes Unrecht vertiefen,[146] läuft er Gefahr, sich zu seinem eigenen rechtsstaatlichen Anspruch in Widerspruch zu setzen.

---

[141] *Nettesheim* (Fn. 121), 39.

[142] Vgl. dazu auch die Überlegungen zu einem „Rote-Linien-Gesetz“: BMI, Datenschutz im Internet – Gesetzentwurf des BMI zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht vom 1.12.2010, S. 2 ff., abrufbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.html;jsessionid=8072D26EC6E674EFBA8D9888F570838A.2_cid287?nn=3314802 (26.4.2016). Dazu auch *Klas* (Fn. 93), S. 57.

[143] So etwa *Wedde* (Fn. 123), § 28, Rdnr. 58.

[144] Für das Landesrecht siehe insofern auch Fußn. 121.

[145] Anders aber *Hackenberg*, Teil 16.7 – Big Data, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, 43. Erg.-Lfg., 2016, Rdnr. 32. Aus dem Widerspruch erwächst nur, aber immerhin ein Verarbeitungsverbot für denjenigen, der die Daten öffentlich gemacht hat (soweit das schutzwürdige Interesse des Betroffenen überwiegt). Zum Löschungs- bzw. Widerspruchsrecht nach § 20 Abs. 2 Nr. 2 und Abs. 5 Satz 1 bzw. § 35 Abs. 2 Nr. 3 und § 35 Abs. 5 Satz 1 BDSG (pro futuro: Art. 17 Abs. 1 lit. c, Abs. 2 i. V. mit Art. 6 Abs. 1 lit. e DSGVO) siehe unten III. 2. d. bb., S. 43.

[146] *Spindler/Nink* (Fn. 131), § 28 BDSG, Rdnr. 12; *ULD Schleswig-Holstein* (Fn. 123), S. 168; *Weichert*, DuD 2009, 7 (11 f.).

Der richtige dogmatische Ort, rechtswidrige Erhebungsursprünge und das fehlende Einverständnis des Betroffenen mit der Veröffentlichung zu berücksichtigen, ist aber nicht das Tatbestandsmerkmal der allgemeinen Zugänglichkeit, sondern die Interessenabwägung des § 14 Abs. 2 Nr. 5 BDSG a. E.[147] Ob der Betroffene mit der Veröffentlichung des Datums einverstanden ist oder ob die öffentliche Zugänglichmachung rechtswidrig war, ändert an der allgemeinen Zugänglichkeit des Datums nämlich nichts: Solange die Daten für jedermann ohne größere, ihrerseits Rechtsgebote verletzende[148] erkennbare Zugangshindernisse abrufbar sind, erfüllen sie die begrifflichen Voraussetzungen des § 14 Abs. 2 Nr. 5 BDSG. Nur eine solche offene Begriffsdeutung trägt auch dem Umstand sachgerecht Rechnung, dass für den Nutzer eines für jedermann zugänglichen Datums nicht ohne unzumutbaren Aufwand erkennbar ist, ob der Betroffene mit der Nutzung auch tatsächlich einverstanden ist.[149] Auch wer eine Aussage aus einer Tageszeitung übernimmt, muss nicht hinterfragen, ob der Betroffene gegen die Auswertung der Informationen Einwände hat. Die Datenauswertung aus öffentlich zugänglichen Daten entartete andernfalls zu einem Spießrutenlauf.

Dem Nutzer das Risiko der Authentizität eines Datums durch eine Prüfpflicht aufzuerlegen, wäre nicht zuletzt auch deshalb unangemessen, weil der Gesetzgeber an die unbefugte Verarbeitung nicht allgemein zugänglicher Daten eine Bußgeldsanktion knüpft (§ 43 Abs. 2 Nr. 1 BDSG)[150]. Rechtfertigbar und inhaltlich nachvollziehbar ist eine solche Sanktion nur dann, wenn der Verarbeiter allgemein zugängliche von sonstigen Daten nach objektiven Maßstäben zweifelsfrei abgrenzen kann. Über Daten, bei denen der Nutzer davon ausgehen darf, dass sie für jedermann – wenn auch nach Anmeldung oder Entrichtung eines Entgelts – zugänglich sind, soll nach der Intention des Gesetzgebers nicht das Damoklesschwert einer Bußgeldsanktion schweben. Dafür sanktioniert die Rechtsordnung im Gegenzug die unbefugte Bereithaltung nicht allgemein zugänglicher Daten zum Abruf mittels automatisierten Verfahrens scharf: Sie belegt dies mit einem Bußgeld (§ 43 Abs. 2 Nr. 2 BDSG), da der Nutzer in diesem Falle weiß, dass er sich den Zugang zu den Daten in unzulässiger Weise erschlichen hat. Die legislative Sanktionsandrohung will

---

[147] Siehe hierzu unten III. 2. c. bb., S. 39. Zu weitgehend daher *Wedde* (Fn. 123), § 28, Rdnr. 58; wie hier *ULD Schleswig-Holstein* (Fn. 123), S. 128.

[148] Darin liegt der Unterschied zu solchen Fällen, in denen sich ein Nutzer unter Überwindung rechtlicher Zugangshürden, z. B. unter Verstoß gegen Nutzungsbedingungen, den Zugang zur Information verschafft. Dazu oben III. 2. c. aa. (1), S. 34.

[149] Ebenso, wenn auch in urheberrechtlichem Kontext, hinsichtlich des Begriffs „öffentlicher Zugänglichmachung“ etwa Schlussantrag des Generalanwalts *Wathelet* vom 7.4.2016 – GS Media –, ECLI:EU:2016:221, Rdnr. 45. Zu weitgehend demgegenüber die Forderung von *Klas* (Fn. 93), S. 70.

[150] Die landesrechtlichen Datenschutzgesetze sehen vergleichbare Sanktionierungen vor, siehe pars pro toto § 41 Abs. 1 Satz 1 Nr. 1 NRWDSG. Hessen sanktioniert ein solches Verhalten demgegenüber nur, wenn es mit Bereicherungsabsicht oder gegen Entgelt erfolgt (§ 40 Abs. 1 Nr. 1 HDSG).

verhindern, dass vertrauliche Daten ohne Befugnis allgemein zugänglich gemacht werden und sich daran zulässige Verarbeitungsvorgänge Dritter knüpfen können – denn was einmal in die Öffentlichkeit gelangt ist, findet den Weg nicht mehr zurück – zum im schlimmsten Fall unwiderruflichen *Orwell*'schen Schaden Betroffener: „Und wenn alle anderen die […] verbreitete Lüge glaubten, wenn alle Aufzeichnungen gleich lauteten, dann ging die Lüge in die Geschichte ein und wurde Wahrheit".[151]

β) Zwischenergebnis

Das Auswertungsprivileg für allgemein zugängliche Daten beschränkt das Gesetz nicht auf rechtmäßig erhobene und mit Zustimmung des Betroffenen veröffentlichte Daten. Auch das, was Betroffene nicht zur allgemeinen Veröffentlichung autorisiert haben, ist allgemein zugänglich.[152]

(3) Zusammenführung verschiedener öffentlich zugänglicher Daten

Durch das Verschneiden allgemein zugänglicher Einzeldaten aus verschiedenen Quellen können völlig neue Informationsbilder entstehen. Dann stellt sich die Frage, ob auch solche Sekundärinhalte, die aus der Kombination allgemein zugänglicher Einzelinformationen entspringen, an dem Privileg der Befreiung von der Zweckbindung teilhaben, das § 14 Abs. 2 Nr. 5 BDSG gewährt – oder ob diese die Daten ausschließlich in ihrem Urzustand erfasst.[153]

α) Persönlichkeitssensibilität der Zusammenführung

Eine Beschränkung auf ihren „ursprünglichen Aggregatzustand" kommt in der Definition des § 10 Abs. 5 Satz 2 BDSG ebenso wenig zweifelsfrei zum Ausdruck wie in § 14 Abs. 2 Nr. 5 BDSG. Die verfassungsrechtliche Gewährleistung der Informationsfreiheit scheint prima facie sogar zu gebieten, in den Genuss einer Privilegierung alles kommen zu lassen, was sich aus allgemein zugänglichen Quellen generieren lässt. Jedoch erstreckt sich ihre grundrechtliche Zweckbestimmung nur auf die Originale einer Information, nicht aber auf eine aus ihnen neu zusammengesetzte Collage; behördlichem Social Media Monitoring kommt diese grundrechtliche Gewährleistung ohnedies nicht zugute.

Je mehr sich das Ergebnis eines Auswertungsprozesses von dem Datum entrückt, das allgemein zugänglich ist bzw. jemand selbst über sich freigegeben hat, und je weniger der Einzelne die Folgen einer Weiterverarbeitung überblicken kann, umso stärker fällt die davon ausgehende

---

[151] *Orwell*, Neunzehnhundertvierundachtzig, 21. Aufl., 1973, S. 34.
[152] Ob die allgemeine Zugänglichmachung autorisiert erfolgte, ist aber bei der Interessenabwägung zu berücksichtigen. Dazu sogleich III. 2. c. bb., S. 39.
[153] In diesem Sinne *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 28, Rdnr. 31; *Simitis*, in: ders. (Hrsg.), BDSG, 8. Aufl., 2014, § 28, Rdnr. 164.

Beeinträchtigung des informationellen Selbstbestimmungsrechts aus. Diejenigen Informationen, die aus der Verknüpfung von Social Media-Daten entstehen, also das Auswertungsergebnis, stellt der Betroffene insbesondere nicht als solche als Informationssubstrat bewusst und damit selbstbestimmt zur Verfügung; sein (etwaiger) Veröffentlichungswille bezieht sich regelmäßig lediglich auf das Einzeldatum.[154] Die Zusammenführung und kontextfremde Verwendung verschiedener allgemein zugänglicher Daten generiert ein im Verhältnis zu den Ausgangsdaten neues Datum.

Welch eindrückliches Mosaik aus Informationen sich durch eine Verknüpfung einzelner Bausteine generieren lässt, ist dem Einzelnen häufig nicht bewusst. Die Funktionalität eines Social Media Monitoring-Algorithmus erschließt sich einem Betroffenen nicht ohne Weiteres – ihm fehlt dazu regelmäßig nicht nur der Sachverstand; bei proprietärer Software ist ihm ein Einblick auch faktisch unmöglich. Gleichzeitig wohnt der Verschneidung von Daten zu einer Collage eine besondere Sensibilität für das informationelle Selbstbestimmungsrecht Betroffener inne, die ein eigenständiges datenschutzrechtliches Kontrollbedürfnis auslösen kann.[155] Das durch ein Social Media Monitoring hervorgebrachte neue Datum ist also nicht als solches allgemein zugänglich. Die Verarbeitungserlaubnis für allgemein zugängliche Daten beschränkt sich folglich grundsätzlich auf die aus der konkreten Quelle stammenden Daten, wie sie in ihrem dort veröffentlichten Zustand vorgelegen haben.[156]

Die historische Auslegung stützt diesen Befund: Das BDSG aus dem Jahre 1977 privilegierte die Verarbeitung allgemein zugänglicher Daten (durch nicht-öffentliche Stellen) nur in ihrem unmittelbar zugänglichen Gehalt. Dort hieß es in § 32 Abs. 1 Satz 2 (ähnlich auch in§ 23 Satz 2): „Abweichend von Satz 1 ist das Speichern zulässig, soweit die Daten *unmittelbar*[157] aus allgemein zugänglichen Quellen entnommen sind“. Die seinerzeit umstrittene Wendung sollte nach dem Willen des Gesetzgebers verhindern, dass Daten allgemein zugänglichen Quellen entnommen, in verschiedenen Dateien gespeichert und durch Verknüpfung mit anderen Informationen zu einem umfassenden Persönlichkeitsdossier zusammengefügt werden können.[158] Die Novelle aus dem Jahr 1990 ließ die ausdrückliche Beschränkung der Privilegierung auf unmittelbar allgemein zugängliche Daten ohne nähere Begründung entfallen.[159] Es handelte sich wohl um eine rein redaktionelle

---

[154] Vgl. auch *Gola/Klug/Körffer* (Fn. 151), § 28, Rdnr. 31; *Richter*, DÖV 2013, 961 (964).
[155] In diesem Sinne wohl *Simitis* (Fn. 151), § 28, Rdnr. 147 ff.; siehe auch *Martini*, DVBl. 2014, 1481 (1489).
[156] *ULD Schleswig-Holstein* (Fn. 123), S. 129; entsprechend eröffnet die Weitergabe personenbezogener Daten an Dritte einen neuen Verwendungszweck und bedarf daher einer eigenen Rechtsgrundlage (§ 28 Abs. 5 BDSG); *Ulmer*, RDV 2013, 227 (230).
[157] Hervorhebung d. Verf.
[158] Vgl. BT-Drucks. 7/1027, S. 22 zu § 2 Abs. 2 Satz 1 des Regierungsentwurfs, welchen das spätere Gesetzgebungsverfahren in Einzelvorschriften überführte (vgl. BT-Drucks. 7/5277, S. 5 f.), ohne die grundsätzliche regulatorische Zielsetzung aufzugeben.
[159] Vgl. BT-Drucks. 11 /4306, S. 9 u. 15 ff. sowie BT-Drucks. 17/7235, S. 98.

Änderung, mit der sich keine Änderung des Regelungsgehalts verknüpfen sollte. Privilegiert sind demnach auch nach geltender Rechtlage nur die unmittelbar allgemein zugänglichen Daten – das aus ihrer Zusammenführung entstehende Auswertungsergebnis hingegen nicht.

β) Vereinbarkeit einer Zusammenführung mit der Gesetzessystematik

Ist ein aus allgemein zugänglichen Quellen zusammengesetztes Informationspuzzle auch nicht als solches allgemein zugänglich, unterfällt das sich aus den Einzelteilen ergebende Bild aber dennoch mittelbar dem Verarbeitungsprivileg des § 14 Abs. 2 Nr. 5 BDSG: Die Herauslösung allgemein zugänglicher Informationen aus ihrem ursprünglichen Kontext, um sie in neue Verwendungszusammenhänge zu stellen, liegt nämlich in der Konsequenz der Befreiung von dem Zweckbindungsgrundsatz, die § 14 Abs. 2 Nr. 5 Hs. 1 BDSG gewährt. Nach ihrer Zweckbestimmung deckt die Vorschrift grundsätzlich gerade das Zusammensetzen inkonnexer Daten zu einem Informationsmosaik als neuem Substrat. Dieses istdamit im Ergebnis vom Verarbeitungsprivileg umfasst. Einige Landesdatenschutzgesetze deuten dies zusätzlich dadurch an, dass sie solche Daten privilegieren, die „aus allgemein zugänglichen Quellen *entnommen werden können*“.[160]

bb) Interessenabwägung

Die umfängliche, systematische und automatisierte Auswertung personenbezogener Daten aus unterschiedlichen allgemein zugänglichen Quellen ruft legitime Abwehrinteressen der Betroffenen auf den Plan. Das Gesetz gestaltet diesen Schutz bisher eher schwach aus. Es gewährt der Verarbeitung allgemein zugänglicher Daten grundsätzlich den Vorrang.[161]

(1) Überwiegendes Schutzbedürfnis des Betroffenen

Für unzulässig erklärt der Gesetzgeber die Auswertung allgemein zugänglicher Daten nur dann, wenn das Interesse des Betroffenen das Auswertungsinteresse der Allgemeinheit offensichtlich überwiegt (§ 14 Abs. 2 Nr. 5 Hs. 2 BDSG[162]).[163] Die gesetzlich geforderte Abwägung richtet sich dabei nicht auf das Interesse an der Zulässigkeit der Verarbeitung im Allgemeinen, sondern auf den Respekt vor dem datenschutzrechtlichen Grundsatz der Zweckbindung (§ 14 Abs. 1 Satz 1 BDSG). Die verarbeitende öffentliche Stelle muss sich also fragen: Überwiegt das Persönlichkeitsinteresse

---

[160] Hervorhebung d. Verf.; § 15 Abs. 2 Nr. 7 BWLDSG; Art. 17 Abs. 2 Nr. 8 BayDSG; § 13 Abs. 2 Satz 1 lit. f. BbgDSG; § 12 Abs. 2 Satz 1 Nr. 6 BremDSG; § 13 Abs. 2 Satz 1 Nr. 7 HmbDSG; § 10 Abs. 3 Satz 1 Nr. 5 i. V. mit § 11 Abs. 2 DSG M-V; § 10 Abs. 2 Satz 1 Nr. 2 i. V. mit § 9 Abs. 1 Satz 3 Nr. 5 NdsDSG; § 13 Abs. 2 Satz 1 lit. f NRWDSG; § 13 Abs. 2 Satz 1 lit. f SaarlDSG; § 10 Abs. 2 Nr. 5 DSG LSA; § 13 Abs. 3 i. V. mit § 11 Abs. 2 SchlHLDSG und § 20 Abs. 2 Nr. 5 ThürDSG.

[161] In diese Richtung auch *Simitis* (Fn. 151), § 28, Rdnr. 163.

[162] Für private Stellen: § 28 Abs. 1 Satz 1 Nr. 3 BDSG; restriktiver bei Markt- und Meinungsforschungszwecken: § 30a Abs.1 Satz 1 Nr. 2 BDSG.

[163] Siehe auch *Gola/Klug/Körffer* (Fn. 151), § 28, Rdnr. 31; *Venzke-Caprese* (Fn. 12), 777; *Wolff* (Fn. 133), § 28 BDSG, Rdnr. 88; *ULD Schleswig-Holstein* (Fn. 123), S. 129.

ausnahmsweise das Interesse der öffentlichen Stelle, die allgemein zugänglichen Daten aus ihrem ursprünglichen Erhebungszweck herauszulösen?

In die Abwägung ist einzustellen, zu welchem Zweck und wann die Veröffentlichung erfolgte[164] sowie ob der Betroffene sie selbst vorgenommen hat (vgl. auch die Wertung des § 13 Abs. 2 Nr. 4 BDSG), zugleich jedoch auch, wie stark die Information tatsächlich verbreitet ist, welche nachteiligen Folgen sich für den Betroffenen mit der Verschneidung verbinden, in welcher Tiefe das Monitoring erfolgt und welchen Detailgrad ein sich aus der Datenzusammenführung ergebendes Persönlichkeitsprofil hat.[165] Je persönlichkeitssensitiver die Datenanalyse, desto höher liegen die Hürden für die Rechtfertigung einer Zweckänderung.[166]

Die für Social Media Monitoring-Zwecke erfolgende Herauslösung von Daten aus ihrem ursprünglichen Kontext kann der Betroffene nur dann unterbinden, wenn sein Interesse, die Daten in ihrem ursprünglichen Verwendungskontext zu belassen, besonders schutzwürdig und dieses Interesse für einen unvoreingenommenen und verständigen Durchschnittsbetrachter ohne Weiteres ersichtlich ist.[167] Offensichtlich überwiegt das Schutzinteresse z. B. regelmäßig bei minderjährigen Betroffenen, bei einem Sperrvermerk oder einer entsprechenden technischen Indizierung, etwa via robots.txt[168].[169] Gleiches gilt, wenn die erstmalige Veröffentlichung bereits offensichtlich rechtswidrig war, z. B. weil sie erkennbar ohne eine im Einzelfall rechtlich gebotene Zustimmung des Betroffenen erfolgte.[170]

Die Behörde trifft im Grundsatz freilich keine Prüfpflicht, eine Webseite proaktiv auf rechtswidrige Inhalte zu durchscannen, bevor sie die Informationen in ein Social Media Monitoring einspeist. Erkennt sie jedoch die Rechtswidrigkeit des Ursprungs oder hätte diese sich aufdrängen müssen, schlägt das in der Interessenabwägung zugunsten des von der Verarbeitung Betroffenen durch.

Eine besondere Prüfpflicht trifft die Behörden aber ausnahmsweise im Hinblick auf Daten, deren Verarbeitung geeignet ist, in *besonders sensible Schutzzonen* der Privatsphäre oder anderer Grundrechte einzudringen. Das gilt etwa für eine Kommunikation über sexuelle Fantasien in einem

---

[164] *Venzke-Caprese* (Fn. 12), 777 und 779.

[165] *Albers*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 14 BDSG, Rdnr. 39; *Dammann* (Fn. 104), § 14, Rdnr. 71; für privates Monitoring auch *Venzke-Caprese* (Fn. 12), 777 und 779.

[166] *Venzke-Caprese* (Fn. 12), 779: Bei privaten Stellen hält er die Beteiligung des betrieblichen Datenschutzbeauftragten für „regelmäßig geboten", bei besonders sensiblem Monitoring sogar eine Vorabkontrolle für erforderlich.

[167] OLG Hamburg, Beschluss vom 13.11.2009, MMR 2010, 141 (142); *Bergmann/Möhrle/Herb* (Fn. 129), § 28 BDSG, Rdnr. 267; *Taeger* (Fn. 129), § 28 BDSG, Rdnr. 103 f.

[168] Vgl. dazu Fußn. 126.

[169] *Wedde* (Fn. 123), § 28, Rdnr. 61.

[170] Siehe dazu bereits III 2. c. aa. (2), S. 35 sowie *Eßer*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 14 BDSG, Rdnr. 41 i. V. mit 33; *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl., 2013, § 14 BDSG, Rdnr. 47; *Wedde*, in: Däubler/Klebe/Wedde et al. (Hrsg.), BDSG, 5. Aufl., 2016, § 14, Rdnr. 15.

Forum,[171] die Teilnahme an einer Demonstration,[172] die Ausübung religiöser Praktiken im öffentlichen Raum oder die Wahrnehmung der Meinungsfreiheit im Rahmen einer gesellschaftspolitischen Debatte. Sind diese Daten in einem anmeldepflichtigen Portal ohne erkennbare Zugangshürden hinterlegt, sind sie zwar allgemein zugänglich i. S. d. § 10 Abs. 5 Satz 2 BDSG.[173] Im Lichte der berührten Grundrechte überwiegt aber im Zweifel das Interesse des Betroffenen daran, seine Daten keiner Zweckänderung ausgesetzt zu sehen: Jenseits ihres Erhebungs-, hier also des Veröffentlichungskontextes, darf der Staat diese grundsätzlich nicht auswerten.[174] Folgerichtig nimmt der Gesetzgeber solche besonderen Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG – mit Ausnahme offenkundig selbst öffentlich gemachter Daten – in § 14 Abs. 5 Satz 1 Nr. 1 BDSG von der Privilegierung des § 14 Abs. 2 Nr. 5 BDSG ausdrücklich aus. In allen anderen Fällen darf die öffentliche Stelle allgemein zugängliche Daten aber grundsätzlich auswerten.

(2) Einschränkende Auslegung für öffentliche Stellen im Lichte des Verhältnismäßigkeitsprinzips

Der weit gefasste Tatbestand des § 14 Abs. 2 Nr. 5 BDSG ebnet nach seinem Wortlaut einer systematischen Ausforschung der engeren persönlichen Lebenssphäre den Weg.[175] In einer Welt ubiquitärer Datenverfügbarkeit ist der Einzelne freilich auf besonderen Schutz davor angewiesen, einer panoptischen Überwachung seiner Privatheit ausgesetzt zu sein. Denn eine persistente staatliche Beobachtung privater Persönlichkeitsentfaltung beschränkt die Freiheit, die das informationelle Selbstbestimmungsrecht gewähren will. Wenn der Einzelne nicht absehen kann, in welchen Kontext seine im Netz verbreiteten Informationen gestellt werden und ob sie in ein Persönlichkeitsprofil einfließen, strahlt das unmittelbar negativ auf seine Freiheit zur Selbstdarstellung und -entfaltung aus.[176] Die Privilegierung des § 14 Abs. 2 Nr. 5 BDSG bedarf daher im Lichte des informationellen Selbstbestimmungsrechts, dessen Vorfeldfunktion für die Verwirklichung anderer Grundrechte und des Verhältnismäßigkeitsprinzips einer restriktiven Deutung.[177] Eine ähnliche Sichtweise hat der EuGH in seinem Google-Urteil mit Blick auf die Grundrechte-Charta anklingen lassen.[178]

---

[171] *Sokol/Scholz* (Fn. 125), § 13, Rdnr. 38.
[172] BVerfG, Einstweilige Anordnung vom 17.2.2009, BVerfGE 122, 342 (369 ff., Rdnr. 132); *Nettesheim* (Fn. 121), 35 ff.
[173] Siehe dazu oben III. 2. c. aa. (1), S. 34.
[174] Ausführlich *Sokol/Scholz* (Fn. 125), § 13, Rdnr. 38 m. w. N. So auch *Gola/Klug/Körffer* (Fn. 119), § 13, Rdnr. 18.
[175] Vgl. dazu auch ausführlich *Oermann/Staben* (Fn. 14), 640 ff.
[176] Vgl. auch *Nettesheim* (Fn. 121), 36.
[177] Ebenso *Eßer* (Fn. 168), § 14 BDSG, Rdnr. 41; *Heckmann* (Fn. 168), § 14 BDSG, Rdnr. 65.
[178] Siehe auch EuGH, Urteil vom 13.5.2014 – Google Spain/AEPD –, ECLI:EU:C:2014:317 Rdnr. 80 f.

§ 14 Abs. 2 Nr. 5 BDSG gestattet in seiner Ratio daher, auch wenn er von der Zweckbindung befreit, nicht die Zusammenstellung von Persönlichkeitsprofilen und Personendatenbanken.[179] Der Respekt vor dem informationellen Selbstbestimmungsrecht setzt dem staatlichen Informationsinteresse bei der Auswertung allgemein zugänglicher Daten in sozialen Netzwerken insoweit eine Grenze.[180] Sie zu überschreiten, ist einer Behörde auch dann verwehrt, wenn der Betroffene die systematisch zusammengetragenen Einzeldaten selbst offenbart hat (§ 13 Abs. 2 Nr. 4 BDSG). Das ergibt sich aus dem Abschreckungszusammenhang zwischen staatlicher Profilbildung und den damit verbundenen Ausstrahlungen auf den grundrechtlich geschützten Tätigkeitsbereich.[181] Eine Befugnis zur Daten*erhebung* impliziert insbesondere keine umfängliche *Verwertung*sbefugnis. Auch allgemein zugängliche Daten sind einer Auswertung daher nur insoweit zugänglich, als diese nicht systematisch personenbezogene Daten zu einem Persönlichkeitsprofil zusammenführt und dadurch in die Rekonstruktion eines Lebensbildes mündet.[182] Regelmäßig unzulässig ist es folglich beispielsweise, Persönlichkeitsprofile von Meinungsführern als Teil eines Social Media Monitoring-Regimes anzufertigen.

d) Betroffenenrechte

aa) Benachrichtigungspflichten

Wer von einer Auswertung allgemein zugänglicher Daten betroffen ist, genießt zwar keinen gesteigerten inhaltlichen, sehr wohl aber einen besonderen verfahrensrechtlichen Schutz. Nach dem Willen des Gesetzgebers ist der Betroffene grundsätzlich über die Speicherung sowie die Art der Daten, die Zweckbestimmung, die Verarbeitung und die Nutzung sowie die Identität der verantwortlichen Stelle und unerwartete Übermittlungsempfänger zu benachrichtigen (§ 19a Abs. 1 Satz 1 u. 2 BDSG[183] [bzw. für private Stellen § 33 Abs. 1 BDSG]; pro futuro: Art. 14 Abs. 1-4 DSGVO[184]).

---

[179] *Roggenkamp* (Fn. 104), § 14 BDSG, Rdnr. 13.
[180] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 14, Rdnr. 19; *Wedde* (Fn. 168), § 14, Rdnr. 17.
[181] Der Anwendungsbereich, der dem § 13 Abs. 2 Nr. 4 BDSG verbleibt, ist insoweit im Ergebnis schmal; vgl. auch *Sokol/Scholz* (Fn. 125), § 13, Rdnr. 38.
[182] Vgl. auch BVerfG, Urteil vom 15.12.1983, BVerfGE 65, 1 (61 f.); BVerfG, Urteil vom 2.3.2010, BVerfGE 125, 260 (323 f.); *Nettesheim* (Fn. 121), 36.
[183] Mit Ausnahme Niedersachsens kennen alle Bundesländer eine vergleichbare Benachrichtigungspflicht, siehe z. B. § 12 Abs. 2 Satz 4 NRWDSG. Zum unionsrechtlichen Hintergrund EuGH, Urteil vom 1.10.2015 – Smaranda Bara –, ECLI:EU:C:2015:638, Rdnr. 28 ff.
[184] Sie begründet insbesondere eine Pflicht zur Information über den Namen und die Kontaktdaten des Verantwortlichen sowie des Datenschutzbeauftragten (Abs. 1 lit. a und b), die Verarbeitungszwecke (Abs. 1 lit. c), die Dauer der Speicherung (Abs. 2 lit. a), die (öffentlich zugängliche) Quelle, aus der die personenbezogenen Daten

Sollte diese Benachrichtigungspflicht auch das Social Media Monitoring in all seinen personenbezogenen Ausgestaltungsformen erfassen, käme das womöglich seinem Abgesang gleich. Der Gesetzgeber ordnet die Benachrichtigungspflicht jedoch nicht vorbehaltlos an: Erfordert die Benachrichtigung einen, etwa mit Blick auf die Zahl der betroffenen Fälle, unverhältnismäßigen Aufwand, ist die verantwortliche Stelle von der Unterrichtung entbunden (§ 19a Abs. 2 Nr. 2 BDSG[185] [bzw. für private Stellen § 33 Abs. 2 Satz 1 Nrn. 7 lit. a, 8 lit. a[186] und 9[187] BDSG]; pro futuro: Art. 14 Abs. 5 lit. b DSGVO). Technisch lassen sich automatisierte elektronische Mitteilungen in ein Social Media Monitoring-Tool zwar im Grundsatz recht leicht und kostengünstig implementieren. Für die Ermittlung zugehöriger Kontakt-, insbesondere E-Mail-Adressen gilt das jedoch typischerweise nicht in gleicher Weise, sondern nur dann wenn jedermann die fraglichen Profile zulässigerweise unmittelbar ansteuern und mit Nachrichten bespielen kann. Den Behörden eine allgemeine Adressermittlung für allgemein zugängliche Quellen aufzuerlegen, wäre im Regelfall unverhältnismäßig. Die verantwortliche Stelle trifft dann aber eine Dokumentationspflicht: Sie muss schriftlich festhalten, unter welchen Voraussetzungen sie von einer Benachrichtigung absieht.[188]

bb) Löschungs- und Widerspruchsrecht

Im Wege eines personenbezogenen Social Media Monitorings automatisiert verarbeitete Daten dürfen die verantwortlichen Stellen nicht auf unbegrenzte Dauer vorhalten. Sie müssen diese löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist (§ 20 Abs. 2 Nr. 2 BDSG[189] [bzw. für private Stellen § 35 Abs. 2 Nr. 3 BDSG[190]]; pro futuro: Art. 17

---

stammen (Abs. 2 lit. f), das Bestehen einer automatisierten Entscheidungsfindung samt aussagekräftiger Informationen über die involvierte Logik sowie die Tragweite der Auswirkungen der Verarbeitung (Abs. 2 lit. g) und Informationen über eine beabsichtigte Weiterverarbeitung zu anderen Zwecken (Abs. 4). Dem Betroffenen steht auch ein Recht auf Auskunft zu (Art. 15 Abs. 1 lit. g) – selbst dann, wenn (wie im Falle von Social Media Monitoring) die personenbezogenen Daten nicht direkt bei ihm erhoben worden sind. Es läuft aber regelmäßig leer, wenn der Betroffene nicht aufgrund einer Benachrichtigung von der Verarbeitung erfährt (vgl. dazu oben im Text).

[185] Mit Ausnahme Berlins, Hessens, Nordrhein-Westfalens und Mecklenburg-Vorpommerns kennen alle Landesdatenschutzgesetze vergleichbare Vorschriften, siehe z. B. § 19 Abs. 2 Satz 1 Nr. 3 RhPfLDSG.

[186] Soweit die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert worden und aus allgemein zugänglichen Quellen entnommen sind, erstreckt sich die Befreiung von der Benachrichtigungspflicht nur auf diejenigen Fälle, in denen die Betroffenen die Daten selbst veröffentlicht haben.

[187] Vgl. hierzu *Stollhoff*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 33 BDSG, Rdnr. 34, 38, 40.

[188] Vgl. etwa *Meents/Hinzpeter*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl., 2013, § 33 BDSG, Rdnr. 59.

[189] Die Datenschutzgesetze der Länder sehen entsprechende Regelungen vor, siehe etwa § 19 Abs. 3 Satz 1 lit. b NRWDSG.

[190] § 35 Abs. 6 BDSG bekräftigt zwar mittelbar, dass die Betroffenenrechte auch bei allgemein zugänglichen Daten grundsätzlich Anwendung finden. Wenn allgemein zugängliche Daten zu Dokumentationszwecken gespeichert werden, ist ihre Berichtigung, Sperrung oder Löschung (entgegen dem Grundsatz des § 35 Abs. 2 Satz 2 BDSG) auch im Falle ihrer Unrichtigkeit oder bestrittenen Richtigkeit aber grundsätzlich ausgeschlossen. Außer bei sensiblen personenbezogenen

Abs. 1 lit. a DSGVO[191]). Daneben steht dem Betroffenen sowohl bei Verarbeitungen privater als auch öffentlicher Stellen das Recht zu, der Verarbeitung zu widersprechen, sofern sein Interesse wegen seiner besonderen persönlichen Situation überwiegt (§ 20 Abs. 5 Satz 1 BDSG[192] [bzw. für private Stellen § 35 Abs. 5 Satz 1 BDSG][193]; pro futuro [mit einer Umkehrung der Vorrang-Vermutung zugunsten des Betroffenen]: Art. 21 Abs. 1 Satz 1 DSGVO[194]]). Von einer Verarbeitung wird der Betroffene im Zweifel freilich kaum erfahren. Er kann der Verarbeitung aber auch proaktiv, etwa durch technische Indizierung oder Konfiguration der Nutzungseinstellungen, entgegenwirken. Entsprechende Möglichkeiten vorzuhalten, legt die DSGVO den Anbietern sozialer Netzwerke konsequenterweise für die Zukunft auf (Art. 21 Abs. 5 i. V. mit Art. 4 Nr. 25 DSGVO i. V. m. Art. 1 Nr. 1 lit. b Richtlinie [EU] 2015/1535). Löschungs- und Widerspruchsrecht sind integraler Bestandteil des Rechts des Einzelnen, nicht an überholten Persönlichkeitsbildern festgehalten zu werden. Das „Recht auf Vergessenwerden“ des Art. 17 DSGVO verleiht diesem Grundprinzip – im Gefolge des Google-Urteils des EuGH[195] – besonderen normativen Flankenschutz. Aber nicht nur derjenige, der wie Google personenbezogene Daten als Intermediär auf einer Plattform öffentlich macht, sollte einer besonderen Informationsverantwortung unterliegen (Art. 17 Abs. 2 DSGVO), sondern de lege ferenda jedenfalls klarstellend auch derjenige, der sie professionell als Teil eines Monitorings verarbeitet. Einer Überholung von Daten durch Zeitablauf bei der Verarbeitung von Daten im Rahmen eines Social Media Monitorings hat die öffentliche Stelle bereits jetzt im Rahmen der Interessenabwägung als schutzwürdiges Interesse des Betroffenen Rechnung zu tragen, soweit sich dies für ihn aus den Informationsbeständen erschließt.

IV. Ausblick auf das nach Inkrafttreten der DSGVO geltende Regelungsregime

Die DSGVO soll die noch aus dem Lochkartenzeitalter stammende Datenschutzregulierung den Herausforderungen des digitalen Zeitalters anpassen. Zwar betont das als digitales Manifest für das 21. Jahrhundert gefeierte Regelwerk die besondere Sensibilität ubiquitärer Datenverfügbarkeit für den Persönlichkeitsschutz sowie einer Überwachung öffentlich zugänglicher Bereiche für die

---

Daten (§ 32 Abs. 2 Satz 2 Nr. 2 BDSG) besteht lediglich ein Recht auf eine Gegendarstellung (§ 35 Abs. 6 Satz 1 und 2 BDSG).

[191] Das Recht auf Löschung greift nach lit. b und c grundsätzlich auch dann, wenn der Betroffene widerspricht oder die personenbezogenen Daten unrechtmäßig verarbeitet worden sind; siehe dazu auch oben III. 2. b. aa. (2), S. 29.

[192] Die landesrechtlichen Datenschutzgesetze halten vergleichbare Regelungen vor, siehe etwa § 4 Abs. 5 NRWDSG. Für einzelne Aufgabenbereiche, etwa Gefahrenabwehr und Steuerfahndung, sehen manche Datenschutzgesetze ausdrücklich Bereichsausnahmen vor, z. B. § 29 Abs. 2 SchlHLDSG.

[193] Vgl. hierzu *Venzke-Caprese* (Fn. 12), 778.

[194] In diesem Fall erwächst dem Betroffenen ein Löschungsrecht gegenüber dem Verantwortlichen (Art. 17 Abs. 1 lit. c DSGVO).

[195] EuGH, Urteil vom 13.5.2014 – Google Spain/AEPD –, ECLI:EU:C:2014:317; dazu etwa *Karg*, ZD 2015, 359 ff.; *Nolte*, NJW 2014, 2238 (2240).

Privatsphäre (vgl. ErwGrd 6 Satz 3 DSGVO). Eine spezielle Regelung für das Social Media Monitoring trifft es hingegen nicht. Auch eine dem Privilegierungstatbestand des § 14 Abs. 2 Nr. 5 bzw. § 28 Abs. 1 Satz 1 Nr. 3 BDSG exakt entsprechende Vorschrift kennt die DSGVO nicht.

Nur an zwei Stellen rekurriert sie in ihrem verfügenden Teil [196] selbst begrifflich auf die Pflichtenstellung desjenigen, der „öffentlich zugängliche Quellen" bzw. „öffentlich gemachte" Daten verarbeitet: In Art. 14 Abs. 2 lit. f legt sie demjenigen eine Unterrichtungspflicht auf, der Daten erhebt, welche aus „öffentlich zugänglichen Quellen" stammen. [197] Daraus lässt sich jedenfalls mittelbar bereits schließen, dass die Verordnung eine Verwertung allgemein zugänglicher Quellen (anstelle einer Direkterhebung bei dem Betroffenen) nicht kategorisch unterbinden will. Für die Verarbeitung besonderer Arten personenbezogener Daten, etwa politischer Meinungen oder der sexuellen Orientierung (Art. 9 Abs. 1 DSGVO), welche die betroffene Person offenkundig selbst öffentlich gemacht hat, wird die Verordnung noch konkreter: Sie nimmt diese Daten von dem grundsätzlichen Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO ausdrücklich aus (Art. 9 Abs. 2 lit. e DSGVO). [198] Für nicht in gleicher Weise sensible Daten, die der Betroffene selbst kundgetan hat (allerdings nur für diese, nicht für solche, welche Dritte über ihn veröffentlicht haben), muss das dann erst recht gelten.

1. Verarbeitungsbefugnisse öffentlicher Stellen

So wenig die Verordnung das Social Media Monitoring selbst einer umfassenden Regelung zuführt, sondern eine solche nur andeutet, so sehr überlässt sie es weitgehend dem Regelungsspielraum der Mitgliedstaaten. Für die Wahrnehmung im öffentlichen Interesse liegender oder in Ausübung öffentlicher Gewalt erfolgender Aufgaben gesteht sie den Mitgliedstaaten in Art. 6 Abs. 1 UAbs. 1 lit. c und b i. V. mit Art. 6 Abs. 2 und 3 DSGVO ausdrücklich umfangreiche Regelungsbefugnisse zu. Dieser Spielraum deckt auch die Auswertung allgemein zugänglicher Quellen ab. Die Verordnung gestattet den Mitgliedstaaten (in den Grenzen des öffentlichen Interesses und der Verhältnismäßigkeit) namentlich, für diese Fälle spezifischere Bestimmungen in ihrem nationalen Recht vorzusehen (Art. 6 Abs. 2 und 3 DSGVO). Auf ihrer Grundlage können (und werden im Zweifel)

---

[196] Vgl. auch ErwGrd 6 Satz 4 DSGVO: „Zunehmend werden auch private Informationen weltweit öffentlich zugänglich."

[197] Demjenigen, der personenbezogene Daten „öffentlich gemacht" hat, legt die Verordnung zusätzliche Pflichten auf. Sie nimmt namentlich die Anbieter sozialer Netzwerke, deren Geschäftsmodell auf eine möglichst umgreifende Verarbeitung personenbezogener Inhalte gerichtet ist, in die Pflicht, um unbeabsichtigte oder nicht mehr erwünschte allgemeine Zugänglichmachungen zu verhindern: Die Voreinstellungen der Diensteanbieter dürfen grundsätzlich nicht mehr eine allgemeine Zugänglichmachung als Grundeinstellung vorsehen (Art. 25 Abs. 2 Satz 3 DSGVO). Sind sie zur Löschung von Inhalten verpflichtet, müssen sie (als Teil des Rechts auf Vergessenwerden) auch Drittverarbeiter über das Löschungsbegehren informieren (Art. 17 Abs. 2 DSGVO); dazu bereits oben III. 2. d., S. 41.

[198] Ebenso für die Verarbeitung besonderer personenbezogener Daten zu präventiv- oder repressiv-polizeilichen Zwecken: Art. 10 lit. c RL 2016/680/EU (Fußn. 76).

Bund und Länder die Vorschrift des § 13 Abs. 2 Nr. 4 und des § 14 Abs. 2 Nr. 5 BDSG bzw. ihre landesrechtlichen Äquivalente[199] weitgehend aufrechterhalten.

2. Verarbeitungsbefugnisse nicht-öffentlicher Stellen

Anders als für öffentliche Stellen behält sich die DSGVO für nicht-öffentliche Stellen die Regelungsbefugnis grundsätzlich selbst vor. Ein Social Media Monitoring findet seine Stütze dann (abgesehen von einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO) regelmäßig lediglich in der Wahrung berechtigter Interessen des für die Verarbeitung Verantwortlichen (Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO).[200] Diese (für rechtssicheren Vollzug) auf eine Konkretisierung durch weiteres Unionsrecht angelegte und angewiesene Generalklausel weist eine hohe Ähnlichkeit zu § 28 Abs. 1 Nr. 2 BDSG auf: Sie lässt eine Verarbeitung des Verantwortlichen zur Wahrung berechtigter Interessen grundsätzlich zu. Wirtschaftliche Auswertungsinteressen des Social Media Monitorings können solche berechtigten Interessen markieren. Die Verordnung stellt sich ihnen nur in den Fällen in den Weg, in denen ausnahmsweise das Persönlichkeitsinteresse des Betroffenen überwiegt (Art. 6 Abs. 1 UAbs. 1 lit. f, Abs. 2 Hs. 2 DSGVO). Diesen grundsätzlichen Vorrang des Auswertungsinteresses betont sie zudem dadurch, dass – im Falle der Weitergabe von Daten – auch die berechtigten Interessen *„eines Dritten“*[201] eine Verarbeitung rechtfertigen können.

An versteckter Stelle gesteht die DSGVO den Mitgliedstaaten jedoch womöglich einen Regelungsspielraum zur Konkretisierung des unionsrechtlichen Rechtsrahmens zu: Sie legt den Mitgliedstaaten die Aufgabe und Befugnis auf, den Konflikt zwischen dem informationellen Selbstbestimmungsrecht sowie der Informationsfreiheit durch gesetzliche Regelungen aufzulösen (Art. 85 Abs. 1 DSGVO). Social Media Monitoring ist ein Paradefall einer solchen regulatorischen Konfliktlage. Wie die Mitgliedstaaten die Gewichtung zwischen den konkurrierenden Positionen vornehmen, obliegt bei weitem Verständnis der Norm der Abwägung der Mitgliedstaaten (in den Grenzen der nationalen und unionalen Grundrechte) . Das schließt dann auch das Recht ein, Verarbeitungsgrundlagen zu erlassen, welche den allgemeinen Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO konkretisierend ausfüllen. Insoweit versteht sich Art. 85 Abs. 1 DSGVO dann als Lex specialis zu Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Ob der deutsche Gesetzgeber auf dieser Grundlage diejenigen Normen, welche das Social Media Monitoring nicht-öffentlicher Stellen anleiten (§ 28 Abs. 1 Satz 1 Nr. 3; § 29 Abs. 1 Satz 1 Nr. 2; § 30a Abs. 1 Satz 1 Nr. 2 BDSG) aufrechterhalten darf, ist aber zweifelhaft. Denn bei genauerem Hinsehen entpuppt sich Art. 85 Abs. 1 DSGVO nicht als Öffnungsklausel. Das machen die innere Systematik der Vorschrift sowie der ErwGrd 153 Satz 1 DSGVO deutlich: Art. 85 Abs. 2 DSGVO lässt mitgliedstaatliche Ausnahmen von

---

[199] Siehe das in Fußn. 121 zitierte Landesrecht sowie Fußn. 112.

[200] Für die Aufgabenwahrnehmung von Behörden schließt die DSGVO die Berufung auf diesen Tatbestand berechtigter Interessen aber ausdrücklich aus (Art. 6 Abs. 1 UAbs. 1 lit. f Satz 2 DSGVO). Für die in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung ist vielmehr alleine Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO einschlägig.

[201] Hervorhebung d. Verf.; Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO.

Regelungen der Verordnung nur für spezifische, insbesondere journalistische Zwecke zu – für alle anderen Zwecke e contrario nicht.
Das Schutzniveau für personenbezogene Daten legt die DSGVO insoweit vielmehr abschließend fest. Art. 85 Abs. 1 DSGVO gibt den Mitgliedstaaten lediglich auf, ihre „Vorschriften über die freie Meinungsäußerung und die Informationsfreiheit“ an diese Vorgaben anzupassen. So bringt es auch ErwGrd 153 Satz 1 DSGVO zum Ausdruck. Eine Deutung der Norm als Öffnungsklausel unterliefe das fein ziselierte Regelungssystem der Verordnung. Nicht zuletzt wäre nicht recht erklärlich, warum Art. 85 Abs. 3 DSGVO den Mitgliedstaaten eine Meldepflicht nur für Ausnahmen nach Abs. 2, nicht aber für (die inhaltlich weiter greifenden) Regelungen nach Abs. 1 auferlegt. Für private Stellen regelt die DSGVO die Zulässigkeit von Social Media Monitoring mithin grundsätzlich selbst, bewegt sich inhaltlich aber in der Rechtskontinuität der bisherigen mitgliedstaatlichen Datenschutzregimes.

3. Abgleich des gegenwärtigen mit dem künftigen nationalen sowie unionalen Rechtsregime

a) Unterschiede

Unterzieht die DSGVO die Zulässigkeit des Social Media Monitorings auch keinem grundlegenden normativen Wandel, weicht sie doch in einem nicht ganz unerheblichen Aspekt von dem heutigen BDSG ab: Sie kennt keine Regelung, die dem Direkterhebungsgrundsatz des § 4 Abs. 2 BDSG in Reinform entspricht. Art. 13 und Art. 14 DSGVO stellen die Erhebung bei dem Betroffenen und bei Dritten vielmehr selbstständig nebeneinander. Das lockert die Daumenschrauben für den Einsatz von Social Media Monitoring ein Stück weit.[202] Gleichzeitig treffen den Verantwortlichen aber immerhin weitreichendere Informationspflichten, wenn er Daten nicht bei der betroffenen Person selbst erhebt (vgl. insbesondere Art. 14 Abs. 2 lit. f DSGVO). Sie sind eine besondere Ausformung des Transparenzgrundsatzes, den Art. 5 lit. a DSGVO etabliert: Der Verantwortliche ist verpflichtet, die Daten in für die betroffene Person *nachvollziehbaren Weise* zu verarbeiten. Der Einzelne soll rekonstruieren können, auf welcher Grundlage und in welchem Umfang wer seine personenbezogenen Daten erarbeitet. Das Transparenzgebot ist mit dem Grundsatz der Direkterhebung nicht deckungsgleich, aber Ausfluss seines Grundgedankens. Es ist auch der Auslegung der einzelnen Erlaubnistatbestände des Art. 6 DSGVO und der „öffentlich zugänglichen Quelle“ in Art. 14 Abs. 2 lit f. DSGVO als Ausgestaltungsmaxime zu unterlegen. Social Media Monitoring kann demnach unzulässig werden, wenn der Betroffene nicht mehr nachvollziehen kann, wie die aus der Analyse hervorgegangenen Informationen und Auswertungsergebnisse, insbesondere korrelationsbasiert ermittelte Wahrscheinlichkeiten, zustande kommen. Dies deutet auch die normative Wertung des Art. 14 Abs. 2 lit. g DSGVO – allerdings beschränkt auf vollständig automatisierte *Entscheidungs*findungen – an.

[202] Das gilt jedenfalls für die Verarbeitung öffentlicher Stellen. Nicht-öffentliche Stellen befreien die Verarbeitungsgrundlagen schon bisher von dem Direkterhebungsgrundsatz; vgl. dazu oben III. 2. b. aa. (1), S. 27.

Dem gleichen Schutzgedanken – den Einzelnen nicht lediglich zum Objekt eines Verarbeitungsprozesses herabzuwürdigen, sondern ihm die Selbstbestimmung über seine Daten zu gewährleisten – ist auch der Zweckbindungsgrundsatz verschrieben (Art. 5 Abs. 1 lit. b DSGVO): Daten sollen grundsätzlich nur Zielsetzungen zugeführt werden, die sich mit den Zwecken vereinbaren lassen, für welche sie ursprünglich erhoben worden sind. Ob eine der Erhebung zugrunde liegende Zielsetzung einer späteren Auswertung entgegensteht, beantwortet das neue Unionsrecht jedoch wohl geringfügig liberaler als das deutsche Recht. Es ist nicht länger erforderlich, dass der Zweck der Weiterverarbeitung dem ursprünglichen Erhebungszweck entspricht (vgl. etwa § 28 Abs. 5, §§ 31 und 39 BDSG, § 78 Abs. 1 Satz 1 SGB X). Es genügt, dass er mit ihm nicht unvereinbar ist, ihm also nicht entgegensteht (ErwGrd 50 Satz 1; Art. 5 Abs. 1 lit. b; Art. 6 Abs. 4 DSGVO). Die Mitgliedstaaten dürfen auch die Herauslösung von Daten aus dem Zweckkontext, für den sie erhoben worden sind, durch eigene Regelungen gestatten, sofern diese erforderlich und verhältnismäßig sind, um spezifische öffentliche Ziele zu erreichen (Art. 6 Abs. 4 DSGVO i. V. mit Art. 23 Abs. 1 lit. a–g DSGVO), insbesondere zum Schutz der öffentlichen Sicherheit (lit. c) oder für sonstige wichtige Ziele des allgemeinen öffentlichen Interesses eines Mitgliedstaats (lit. e).[203] Die bisherige Befreiung *öffentlicher* Stellen von der Zweckbindung bei der Verarbeitung allgemein zugänglicher Quellen dürfen die Mitgliedstaaten auf dieser Grundlage weiter aufrechterhalten. [204] Bei allgemein zugänglichen Quellen besteht ohnedies in der Regel nur ein loser Zweckzusammenhang: Daten, die rechtmäßig jedermann zugänglich sind, stehen – der Zweckbestimmung der Veröffentlichung entsprechend –für eine Vielzahl von Zwecken zur Verfügung und sind mit ihnen typischerweise vereinbar. Der Zweckbindungsgrundsatz steckt einem Social Media Monitoring daher keine engen Grenzen.

b) Zukunft des Social Media Monitorings zu Profiling-Zwecken

Einer *Verwertung* von Informationen, die auf der Grundlage eines Social Media Monitorings persönliche Aspekte einer Person, etwa die Arbeitsleistung, wirtschaftliche Lage, Gesundheit etc. bewerten (Profiling – Art. 4 Abs. 4 DSGVO), setzt die DSGVO den Verwirklichungsanspruch des Persönlichkeitsrechts entgegen: Eine automatisierte Generierung von Einzelentscheidungen belegt sie (ähnlich wie auch schon § 6a BDSG) grundsätzlich mit einem Verbot (Art. 22 Abs. 1 DSGVO).[205] Es erstreckt sich aber nur auf *Entscheidungen*, die auf Profiling beruhen, verbietet dieses als solches

[203] Für die Zweckänderung bei Daten, die für andere als präventiv- oder repressiv-polizeiliche Zwecke erhoben worden sind, zieht Art. 4 Abs. 2 RL 2016/680/EU (Fußn. 76) die Grenzen noch weiter: Sie bindet die Zweckänderung an das Verhältnismäßigkeitsprinzip. Sollen umgekehrt Daten, die für präventiv- oder repressiv-polizeiliche Zwecke erhoben worden sind, für andere Zwecke verarbeitet werden, gelten die engeren Grenzen des Art. 6 Abs. 4 DSGVO (Art. 9 Abs. 1 Satz 2 RL 2016/680/EU [Fußn. 76]).

[204] Darüber hinaus trifft ihn nach Art. 14 Abs. 4 DSGVO eine Informationspflicht gegenüber dem Betroffenen, wenn er eine zweckverändernde Weiterverarbeitung beabsichtigt.

[205] Für die Verarbeitung personenbezogener Daten zu präventiv- bzw. repressiv-polizeilichen Zwecken: Art. 11 Abs. 1 Richtlinie 2016/680/EU (Fußn. 76).

– anders als die Hervorhebung des Profilings in der Überschrift insinuiert – freilich nicht als *Auswertungsinstrument* mitsamt des ihm ggf. vorgeschalteten Social Media Monitorings. Entscheidungen, welche dem Betroffenen gegenüber rechtliche Wirkung entfalten oder ihn faktisch in einer vergleichbaren Weise nachhaltig beeinträchtigen, dürfen Verarbeiter vielmehr *nicht alleine* auf Profiling stützen. Ein profilbildendes Social Media Monitoring darf folglich lediglich Bestandteil eines Bündels mehrerer Entscheidungsparameter sein. Insbesondere muss eine (nicht nur lediglich formal bestätigende) menschliche Entscheidung dazwischentreten. Dem Geschäftsmodell des Social Media Monitorings, insbesondere seiner Zielsetzung, Profilbilder herzustellen und zu beobachten, setzt das aber ebenso wie die an ein Profiling anknüpfende Informationspflicht (Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO) sowie das Auskunfts- (Art. 15 Abs. 1 lit. h DSGVO) und Widerspruchsrecht (Art. 21 Abs. 1 Satz 1 Hs. 2 DSGVO) Schranken.

Zugleich schließt die Verordnung auch den Einsatz von Profiling-Maßnahmen zum Zwecke des Abschlusses und der Erfüllung von Verträgen – wie schon § 6a Abs. 2 Nr. 1 BDSG – nicht kategorisch aus (Art. 22 Abs. 2 lit. a DSGVO). Auf der Grundlage der Öffnungsklausel des Art. 22 Abs. 2 lit. b DSGVO dürfen die Mitgliedstaaten darüber hinaus – unter Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der Betroffenen – weitere Ausnahmen von dem Verbot automatisierter Einzelentscheidungen zulassen. Für die Vorbereitung von Vertragsschlüssen, etwa Ratenverträgen, zur Darlehensgewährung, zur Kreditauskunft oder zum Abschluss von Arbeitsverträgen wird die Bedeutung von Social Media Monitoring-Maßnahmen auch im neuen europäischen Rechtsrahmen in der Folge eher zu- als abnehmen. Einem ordnungsbehördlichen Profiling zu Zwecken der Abwehr von Gefahren für die öffentliche Sicherheit oder der Bekämpfung von Straftaten setzt die Union aber eine zusätzliche Schranke: Es ist in Zukunft ausdrücklich einem besonderen unionsrechtlichen Diskriminierungsverbot unterworfen, das auf die persönlichkeitsrechtliche Sensibilität der Maßnahme Rücksicht nimmt; nach besonderen Kategorien personenbezogener Daten, wie Rasse oder ethnischer Herkunft, darf ein Monitoring, welches auf die Bewertung persönlicher Aspekte einer Person zielt, nicht diskriminieren (Art. 11 Abs. 3 Richtlinie 2016/680/EU[206]).

V. Rechtspolitische Desiderate und Fazit

Im Methodenrepertoire der Marktforschung hat Social Media Monitoring längst einen Stammplatz erobert. Auch Behörden erschließen sich zusehends seine Nutzungspotenziale. Soweit sich die algorithmengesteuerte Durchforstung sozialer Netzwerke lediglich auf aggregierte und anonymisierte öffentlich zugängliche Massendaten beschränkt, ist das Persönlichkeitsrecht und damit auch das Datenschutzrecht nur bei dem damit einhergehenden Vorgang der Datenerhebung tangiert. Aber auch einem Social Media Monitoring, das Daten ad personam auswertet, ebnet der Gesetzgeber bisher in weitem Umfang den Weg: Über den Hebel „allgemein zugängliche Quelle“

[206] Fußn. 76.

gesteht er ihm eine privilegierte Auswertungsmöglichkeit zu. Dem Informationsinteresse der Allgemeinheit gewährt er damit gegenüber dem Persönlichkeitsinteresse des Betroffenen im Zweifel den Vortritt. Sub specie der Verarbeitung *Privater* ist diese Wertung Ausfluss der verfassungsrechtlich gewährleisteten Informationsfreiheit. *Behörden* können sich auf sie nicht berufen, genießen bei der Auswertung allgemein zugänglicher Quellen im Rahmen ihrer Aufgabenerfüllung aber gleichwohl ein gesetzliches Nutzungsprivileg im Hinblick auf die beim Social Media Monitoring erfolgende Zweckänderung.

1. Verschiebung der informationellen Macht im digitalen Zeitalter

Auf die Herausforderungen, die von einem Social Media Monitoring für den Persönlichkeitsschutz ausgehen, erweist sich das Datenschutzrecht nur unzureichend vorbereitet. Sein regulatorisches Konzept ist noch weithin auf die analoge Welt zugeschnitten. Als die normative Privilegierung für allgemein zugängliche Quellen und ihre weite Definition in § 10 Abs. 5 Satz 2 BDSG entstand, war sie in ihrer ursprünglichen Ausformung uneingeschränkt sachgerecht: Die Möglichkeit, Informationen allgemein zugänglich zu machen, war zu dieser Zeit noch auf eine kleine „Kaste“ von (dem Pressekodex verpflichteten) Medienmachern beschränkt. Entsprechend dachte der Gesetzgeber bei allgemein zugänglichen Quellen noch an Zeitungen, Adressbücher und Fernsprechverzeichnisse.[207] Dass das Web 2.0 es jedermann ermöglicht, der Öffentlichkeit – ohne redaktionelle Kontrolle und nicht nur ohne, sondern auch gegen den Willen Betroffener – entgrenzt von Raum und Zeit Informationen zugänglich zu machen, stand dem Gesetzgeber des BDSG noch nicht vor Augen. Das Smartphone als universelle Zapf- und Einspritzanlage der digitalen Öffentlichkeit, mit dem sich in Sekundenschnelle private Momente fotografieren, intime Gespräche aufzeichnen und in soziale Netzwerke integrieren lassen, sowie die technischen Kapazitäten von Big Data-Algorithmen zur Erstellung von Persönlichkeitsprofilen verschieben das informationelle Gleichgewicht. Folgte die alte Medienwelt noch dem Muster „erst filtern, dann publizieren“, verhält es sich im digitalen Kosmos umgekehrt. Die umfassende Privilegierung allgemein zugänglicher Daten schießt in einer digitalisierten Welt insofern ein Stück weit über das ursprüngliche Ziel und den intendierten Regelungsansatz hinaus.[208] Die vereinfachten Möglichkeiten, Informationen aus ihren ursprünglichen Veröffentlichungskontexten herauszulösen, bergen die Gefahr, die Vielfalt unterschiedlicher Öffentlichkeiten und die damit jeweils verbundenen Schutzbedürfnisse der Betroffenen – insbesondere die kontextuale Zweckbestimmung der erstmaligen

[207] BT-Drucks. 7/1027, S. 22.
[208] Wie hier tendenziell *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 250 f.; a. A. wohl *Nettesheim* (Fn. 121), 39 f.

Informationspreisgabe –, durch eine pauschale Öffnung zur allgemeinen Auswertung aus dem Auge zu verlieren.[209]

2. Handlungsempfehlungen de lege ferenda

Wer Informationen in sozialen Netzwerken hochlädt, muss zwar grundsätzlich mit einer Kenntnisnahme durch eine Vielzahl an Akteuren rechnen. Das heißt aber noch nicht zwingend, dass er diese Informationen auch für jedermann zu unbegrenzten Auswertung freigibt.[210] Erfolgt eine *netzwerköffentliche* Verbreitung in sozialen Netzwerken auch bewusst mit einer Streuwirkung, so ist sie in ihrer inneren Zielrichtung doch zugleich grundsätzlich auf die Community des sozialen Netzwerks begrenzt – nur ihr gilt das Vertrauen, das der Einzelne Nutzungsinteressenten entgegenbringt. Dass sich diese Erwartung leicht enttäuschen lässt und die Informationen zur wirtschaftlichen Auswertung oder zur Befriedigung staatlicher Informationsinteressen nutzen lassen, ist dem Einzelnen nicht immer bewusst. Diese überschießende Tendenz des Nutzungsverhaltens macht sich Social Media Monitoring zunutze, indem es die Abfallprodukte informationeller Selbstdarstellung und Mitteilsamkeit als Sekundärprodukt verwertet. Das heißt jedoch noch nicht zwingend, dass der Einzelne mit einer unter Überwindung von Zugangshindernissen erfolgenden Informationsexploration vorbehaltlos rechnen und sich dies als rechtliche Wertung entgegenhalten lassen muss.[211] In dem grundrechtlich besonders geschützten, durch Authentifizierung gesicherten Handlungsumfeld eines sozialen Netzwerks sollte nicht jedermann gewärtigen müssen, dass die Informationen (z. B. zur Bedürftigkeit eines Hartz IV-Empfängers oder zur beabsichtigten Teilnahme an Demonstrationen) staatlich ausgeleuchtet und nutzbar gemacht werden. [212] Ein soziales Netzwerk kann nur dann zum unbefangenen

---

[209] *Leopold*, Vorgänge 2012, 74 (80).

[210] *Kirchhof*, AIB extra 2015, 6 (14).

[211] A. A. BVerfG, Urteil vom 27.2.2008, BVerfGE 120, 274 (346, Rdnr. 311): „Auch im Rahmen einer solchen Kommunikationsbeziehung ist jedem Teilnehmer bewusst, dass er die Identität seiner Partner nicht kennt oder deren Angaben über sich jedenfalls nicht überprüfen kann. Sein Vertrauen darauf, dass er nicht mit einer staatlichen Stelle kommuniziert, ist in der Folge nicht schutzwürdig." Ebenso *Böckenförde* (Fn. 58), S. 197; *Kudlich* (Fn. 7), 198 f. Wie hier aber in der Tendenz *Biemann* (Fn. 7), S. 137. Ebenso *Schulz/Hoffmann* (Fn. 46), 133 mit Fußn. 24, die ihre Argumentation auf die „Veränderung der Realität, die durchaus lange Beziehungen unter Pseudonymen hervorbringen kann" stützen. Das geänderte Nutzerverhalten im Umgang mit allgemein zugänglichen Daten vor dem Hintergrund eines allgemeinen Wertewandels analysierend *Petri*, DuD 2010, 25 (28 f.).

[212] Das schließt auch die rein verwaltungsinterne Verwendung ein [a. A. wohl *Nettesheim* (Fn. 121), 36]. Gleiches gilt, wenn die Nutzungsbedingungen eines sozialen Netzwerks ausdrücklich die Nutzung der Informationen zu Monitoring-Zwecken ausschließen. Das kann auch auf die Interessenabwägung durchschlagen, vgl. in diesem Sinne auch (für die Recherche des Arbeitgebers über Bewerber) *Klas* (Fn. 93), S. 45 sowie den (inzwischen obsoleten) Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BT-Drucks. 17/4230, S. 16. Letzterer erkannte in diesem Fall ein überwiegendes Interesse des Arbeitnehmers an der Nichtauswertung seiner Daten. Es liegt aber grundsätzlich auch schon kein allgemein zugängliches Datum vor (vgl. dazu oben III. 2. c. aa. (1), S. 34). Denn die rechtswidrige Überwindung von Zugangssicherungen verschafft nicht den Zugang zu allgemein verfügbaren Daten. Öffentliche Stellen

Umschlagplatz von Meinungen und einer Plattform des demokratischen Austausches avancieren, wenn der Homo digitalis die Gefahr der Verletzlichkeit seiner Persönlichkeitsentfaltung im Netz und des Gefühls steten Überwachtwerdens hinreichend wirksam gebannt sieht.[213] Die Chancen einer digitalisierten Welt für das Gemeinwohl und ein diskursives Demokratiemodell wären bedroht, würde der Satz des Alphabet-Vorsitzenden *Eric Schmidt* zur Leitregel allgemeinen Rechts: „Wenn Sie nicht wollen, dass Ihr Tun im Netz missbraucht wird, dann sollten Sie es gar nicht tun."

Im Zweifel ist bei jeglicher Form der Verlautbarung, die für Dritte erst nach erfolgter Authentifizierung (etwa durch Eingabe eines Passworts) sichtbar ist,[214] keine Adressierung der Allgemeinheit gewünscht – ebenso wenig, wenn der Betroffene dies durch Voreinstellungen zur Privatsphäre zu erkennen gibt oder die Informationen zur von der Indexierung durch Suchmaschinen eindeutig ausschließt. Der Begriff der allgemeinen bzw. öffentlichen Zugänglichkeit i. S. d. § 10 Abs. 5 Satz 2 BDSG bzw. des künftigen Datenschutzregimes sollte entsprechend an das Bestimmungsrecht des Trägers der Informationsquelle rückgebunden werden.[215] Es bedarf insbesondere einer Differenzierung zwischen (nur) netzwerköffentlichen und allgemein zugänglichen Daten. Entgegen § 10 Abs. 5 Satz 2 BDSG sollte de lege ferenda der Grundsatz gelten: Nur das, was jemand der *gesamten* Öffentlichkeit zur Verfügung stellt, darf auch jedermann nutzen und auswerten. Die weite Privilegierung für das Social Media Monitoring bedarf daher einer Einschränkung auf Daten, die jedermann ohne vorherige Authentifizierung (wenn auch ggf. nach Entrichtung eines Entgelts) einsehen und nutzen darf.[216] Das ist Ausdruck eines zeitgemäßen Verständnisses der grundrechtlichen Schutzfunktion des Staates für das informationelle Selbstbestimmungsrecht im digitalen Kosmos.[217] In § 10 Abs. 5 Satz 2 BDSG bzw. seiner Nachfolgeregelung sollte mithin der Passus „oder nach vorheriger Anmeldung" gestrichen werden. Damit wäre ein Großteil der Informationen sozialer Netzwerke wie Facebook (in dem nicht ohne Authentifizierung zugänglichen Informationsstrom) nicht allgemein zugänglich: Nur das, was nicht passwortgeschützt, sondern jedermann ohne weitere Einschränkung der Sichtbarkeit, etwa durch den Nutzer selbst oder das Erfordernis einer Gruppenanmeldung, zugänglich ist, also über

---

müssen in Anbetracht entsprechender „schutzfeindlicher" Voreinstellungen in entsprechenden Systemen aber nicht im Zweifel davon ausgehen, dass beim Fehlen von Nutzungsbeschränkungen ein Versehen des Betroffenen vorliegt. Das würde die Schutzpflicht der Behörden überdehnen. In diesem Sinne aber *Wedde* (Fn. 123), § 28, Rdnr. 32.

[213] Siehe dazu auch die Nachweise in Fußn. 71.

[214] Dass die Authentifizierung auch anderen Zwecken, etwa der personenspezifischen Zuordnung von Informationen, dient, ändert daran nichts. A. A. in der Tendenz *Biemann* (Fn. 7), S. 142 f.; *Kudlich* (Fn. 7), 198.

[215] Vgl. zum verfassungsrechtlichen Begriff der Informationsfreiheit etwa BVerfG, Urteil vom 24.1.2001, BVerfGE 103, 44 (60 f., Rdnr. 59 ff.); BVerwG, Beschluss vom 18.7.2011, NVwZ 2011, 1072 (1073, Rdnr. 9).

[216] In diese Richtung *Klas* (Fn. 93), S. 70.

[217] Zur gestiegenen Relevanz des Datenschutzes zwischen Privaten und grundrechtlichem Datenschutz durch Schutzpflichten des Staates siehe *Masing*, NJW 2012, 2305 (2306 ff.). Siehe in diesem Zusammenhang auch *Hoffmann/Schulz/Borchers*, MMR 2014, 89 (89 ff.).

Suchmaschinen für jedermann auffindbar ist, fällt dann unter das Verarbeitungsprivileg der allgemeinen Zugänglichkeit. Ein solches Verständnis läutet dem Social Media Monitoring nicht das Totenglöckchen; vielmehr bringt es das Instrument mit dem Recht auf informationelle Selbstbestimmung in Einklang.[218]

3. Status quo de lege lata

Öffentliche Stellen sind beim Social Media Monitoring aufgrund ihrer Grundrechtsbindung besonderen Schranken unterworfen. Das schließt ihren Zugriff auf für jedermann ohne vorherige Authentifizierung zugängliche Quellen nicht kategorisch aus; für alles, was darüber hinausgeht,sind sie aber auf eine besondere gesetzliche Grundlage angewiesen.[219] Bereits de lege lata stehen ihrer Auswertung weder rechtswidrig erhobene Daten offen[220] noch dürfen sie Social Media-Daten zu personenbezogenen Persönlichkeitsprofilen zusammenführen [221] . Auch der Direkterhebungsgrundsatz des § 4 Abs. 2 Satz 1 BDSG zieht dem Monitoring öffentlicher Stellen Grenzen; [222] die DSGVO wird ihn aber nicht mehr fortführen, sondern ersetzt ihn durch ein Transparenzgebot (Art. 5 lit. a DSGVO).

Unter dem Regime der DSGVO und der Richtlinie 2016/680/EU[223] wird die Bundesrepublik die Verarbeitungserlaubnisse des § 13 Abs. 2 Nr. 4 BDSG (für vom Betroffenen „offenkundig öffentlich gemacht[e]“ Daten) und des § 14 Abs. 2 Nr. 5 BDSG (für „allgemein zugänglich[e]“ Daten) sowie ihre landesrechtlichen Äquivalente [224] aufrechterhalten können – ebenso die spezialgesetzlichen Eingriffsgrundlagen der Polizeigesetze und der StPO (Art. 6 Abs. 2 u. 3 i. V. m Art. 6 Abs. 1 lit. e DSGVO bzw. Art. 4 Abs. 1 und 2 sowie 8 Abs. 1 Richtlinie 2016/680/EU [225]). Der nationale Regelungsspielraum für das Social Media Monitoring öffentlicher Stellen bleibt insoweit auch unter der DSGVO weitgehend erhalten. Zulässig ist und bleibt der Zugriff auf Daten, die Betroffene selbst ohne das Erfordernis vorheriger Authentifizierung (etwa durch Passwortschutz) öffentlich gemacht haben. Nichts anderes gilt für den großen Bereich der Stimmungsbilderhebung auf der Grundlage anonymisierter, aggregierter Massendaten. Denn die Anonymisierung löst den Personenbezug auf

---

[218] Ob das enge Verständnis allgemeiner Zugänglichkeit außer für öffentliche Stellen auch für Private gelten soll, lässt sich rechtspolitisch unterschiedlich werten. Die Folgen der Entscheidung sind rechtspolitisch bedeutsam: Will ein soziales Netzwerk die nur nach einer Authentifizierung sichtbaren Inhaltsdaten seiner Nutzer zur Auswertung für private Dritte freigeben, ist das dann zwar weiterhin möglich. Es ist dazu aber auf eine informierte Einwilligung des Betroffenen angewiesen. Diese muss – insbesondere durch geeignete standardisierte Symbole – klar erkennbar und für den Nutzer verständlich sein (vgl. auch pro futuro Art. 7 Abs. 2 Satz 1 DSGVO).

[219] *Achtruth*, Der rechtliche Schutz bei der Nutzung von Social Networks, 2014.

[220] Siehe dazu oben III. 2. c. aa. (2), S. 35 .

[221] Siehe dazu oben III. 2. c. aa. (3), S. 37.

[222] Siehe dazu oben III. 2. b. aa, S. 28.

[223] Fußn. 76.

[224] Siehe etwa § 12 Abs. 1 Satz 1 und § 13 Abs. 1 Satz 1 NRWDSG.

[225] Fußn. 76.

und befreit die Daten dadurch aus dem Klammergriff des Datenschutzregimes. Sowohl für öffentliche als auch für private Stellen sollte der Normgeber freilich das Gebot frühzeitiger Anonymisierung der personenbezogenen Daten eines Social Media Monitorings – nach dem Vorbild des § 30a Abs. 3 BDSG – ausdrücklich und klarstellend verankern.[226]

4. Gesamtbewertung

Social Media Monitoring ist ein innovatives Instrument der Datenverwertung, dessen ökonomischen Wertschöpfungsgehalt und gesellschaftlichen Ertrag erst die digitalisierte Welt mit ihren technischen Möglichkeiten aus der Taufe heben konnte. Sowohl im privaten als auch im öffentlichen Sektor kann es wichtige Funktionen eines gesellschaftlichen Frühwarnsystems wahrnehmen und digital-vernetzte Partizipationshorizonte erschließen. Zu den Grundprinzipien des Persönlichkeitsschutzes steht es in einem natürlichen Spannungsverhältnis. Auflösen lässt es sich am zielgenauesten, wenn für den Betroffenen stets erkennbar ist, welche seiner digitalen Fußspuren nachverfolgt werden, in die Analyse einfließen und zu welchen Auswertungsergebnissen sie auf welche Weise beitragen. Den verfahrensrechtlichen Auskunfts-, Löschungs- und Widerspruchsrechten[227] kommt insoweit eine wichtige flankierende Sicherungsfunktion zu.

Andernfalls macht Social Media Monitoring den Einzelnen reflexartig zu einem Objekt panoptischer Dauerüberwachung, welche die autonome Selbstentfaltung unter eine undurchsichtige Glocke stiller Abschreckung legt. Die Sorge vor stetiger heimlicher Beobachtung droht der Freiheit dann die Luft abzuschnüren. Gerade im digitalen Morgenland ist eine vom Beobachtungsradius staatlicher und privater Akteure freie Entfaltungszone das Lebenselixier einer demokratischen Gesellschaft. Die Worte des ehemaligen NSA-Chefs *Keith Alexander* „Man braucht den Heuhaufen, um darin die Nadel zu finden," sollte ein dem Datenschutz verschriebener Rechtsstaat daher weniger als Handlungsanleitung im Umgang mit den Datenhalden sozialer Netzwerke verstehen – sondern vielmehr als Warnsignal aus dem Maschinenraum weltumspannender Datenkollektoren. Denn ein Gemeinwesen, das (angelehnt an *Benjamin Franklin*) die Freiheit um der Optimierung staatlicher Aufgabenerfüllung willen aufgibt, läuft Gefahr, am Ende auf beides verzichten zu müssen.

---

[226] Allgemein pro futuro: Art. 25 Abs. 1 DSGVO (Datenschutz durch Technik). Bei der *Beschaffung* eines Social Media Monitoring-Tools ist entsprechend das sog. Drill Down-Niveau, d. h. die mögliche Betrachtungstiefe aggregierter Daten, ein Gradmesser für die Datenschutzkonformität des Werkzeugs. An ihm lässt sich die Qualität der Datenanonymisierung und des De-Anonymisierungsrisikos ablesen. Je detaillierter sich die Datenaggregate und Analyseergebnisse eines Monitorings auf einzelne Social Media-Beiträge und -ereignisse zurückverfolgen lassen, desto wahrscheinlicher enthalten sie Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person und umso größer sind die datenschutzrechtlichen Risiken. Zielt die Analyse auch darauf, Meinungsführer zu identifizieren, ihr Verhalten zu scannen und Profile von ihnen zu erstellen, ist das ein starkes Indiz für eine – unter Big Data-Bedingungen – technisch mögliche De-Anonymisierung.

[227] Dazu oben III. 2. d., S. 43.

Literaturverzeichnis

Achtruth, Björn, Der rechtliche Schutz bei der Nutzung von Social Networks, Münster, 2014.

Anonymous, BND will soziale Netzwerke in Echtzeit ausforschen, Der Bundesnachrichtendienst will künftig live mithorchen, was Nutzer auf Facebook oder Twitter schreiben und posten. Dafür soll der Dienst digital aufgerüstet werden, Zeit Online vom 30.5.2014, http://www.zeit.de/digital/internet/2014-05/bundesnachrichtendienst-soziale-netzwerke-facebook-twitter-spionage (19.11.2015).

– Analysefirma nutzt Zugang zu sozialen Medien für US-Polizei aus, Spiegel Online vom 12.10.2016, http://www.spiegel.de/netzwelt/web/geofeedia-analysefirma-lieferte-polizei-daten-aus-sozialen-netzwerken-a-1116242.html (25.10.2016).

Aßmann, Stephanie/*Pleil*, Thomas, Social Media Monitoring: Grundlagen und Zielsetzungen, in: Zerfaß, Ansgar/Piwinger, Manfred (Hrsg.), Handbuch Unternehmenskommunikation, Wiesbaden, 2007, S. 585–604.

Auernhammer, Herbert (Hrsg.), BDSG, 4. Aufl., Köln, 2014.

Bäcker, Matthias, Grundrechtlicher Informationsschutz gegen Private, Der Staat 2012, S. 91–116.

Baeriswyl, Bruno, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber, Rolf H./Thouvenin, Florent (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich, 2014, S. 51–60.

Bär, Wolfgang, Strafrechtliche Kontrolle in Datennetzen, MMR 1998, S. 463–468.

Bergmann, Lutz/*Möhrle*, Roland/*Herb*, Armin (Hrsg.), Datenschutzrecht, Kommentar Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, bereichsspezifischer Datenschutz, Stuttgart, 50. Erg.-Lfg. 2016.

Beuth, Patrick, Das BKA will in die Zukunft sehen, Zeit Online vom 17.3.2014, http://www.zeit.de/digital/datenschutz/2014-03/bka-data-mining-predictive-policing (19.11.2015).

Biemann, Jens, „Streifenfahrten" im Internet, Die verdachtsunabhängigen Ermittlungen der Polizei im virtuellen Raum, Stuttgart, 2013.

BITKOM, Leitfaden Social Media, 2012, https://www.bitkom.org/Publikationen/2012/Leitfaden/Neue-Auflage-Leitfaden-Social-Media/LeitfadenSocialMedia20121.pdf (3.3.2016).

Böckenförde, Thomas, Die Ermittlung im Netz, Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, Tübingen, 2003.

Bohannon, John, Credit card study blows holes in anonymity, science 347 (2015), S. 468.

Brauckmann, Patrick (Hrsg.), Web-Monitoring, Gewinnung und Analyse von Daten über das Kommunikationsverhalten im Internet, Konstanz, 2010.

Brus, Eva-Maria/*Schwab*, David, Medizinische Einsatzmöglichkeiten von Big Data oder Big Data im Gesundheitswesen - am Datenschutz erkrankt?, in: Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht, 2014, S. 171–182.

Bundesministerium des Innern, Erstes Führungskräftekolleg Polizei und Verfassungsschutz, Die Zusammenarbeit von Polizei und Verfassungsschutz vor dem Hintergrund der Ermittlungen zur "Zwickauer Zelle" stehen im Fokus.,

http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2012/06/fuehrungskraeftekolleg-polizei-verfassungsschutz.html (19.11.2015).

– Leitfaden Krisenkommunikation, Berlin, 2014.

Bundeszentralamt für Steuern, Xpider, http://www.bzst.de/DE/Steuern_International/USt_Betrugsbekaempfung/Internet_Ermittlung/Internet_Ermittlung.html?nn=23442 (25.4.2016).

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. 12–16.

China Copyright and Media, Planning Outline for the Construction of a Social Credit System (2014-2020), https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (19.4.2016).

Däubler, Wolfgang/*Klebe*, Peter/*Wedde*, Peter/Weichert (Hrsg.), BDSG, 5. Aufl., Frankfurt am Main, 2016.

Drüke, Helmut/*Krellmann*, Anika/*Scholz*, Simon/*Veit*, Sylvia, Wie nutzen Kommunen Social Media?, 2016, http://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IBWL/Veit/Publications/Social-Media-Studie2016_cassini-KGSt-UniKassel.pdf (15.12.2016).

Eckhardt, Jens/*Kramer*, Rudi, Auftragsdatenverarbeitung beim Einsatz von Persönlichkeitsanalysetools, DuD 2016, S. 144–149.

Eichenhofer, Johannes, Privatheit im Internet als Vertrauensschutz. Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz, Der Staat 55 (2016), S. 41–67.

Eifert, Martin, Verwaltungskommunikation im Internet, in: Ladeur, Karl-Heinz (Hrsg.), Innovationsoffene Regulierung des Internet, Baden-Baden, 2003, S. 131–154.

– Informationelle Selbstbestimmung im Internet, Das BVerfG und die Online-Durchsuchungen, NVwZ 2008, S. 521–523.

Ernst, Stefan, Social Networks und Arbeitnehmer-Datenschutz, NJOZ 2011, S. 953–958.

Erster Arbeitskreis Socialmedia B2B, B2B und Social Media – Wie verändert sich die Nutzung der Kanäle?, Ergebnisse 6. Studie 2016, München, 2016.

Fischoeder, Christof/*Kirsch*, Robert/*Visser*, Sven/*Leupold*, Jörg, Social Media-Monitoring in der Praxis am Beispiel des Bundestagswahlkampfes 2009, in: Brauckmann, Patrick (Hrsg.), Web-Monitoring, Gewinnung und Analyse von Daten über das Kommunikationsverhalten im Internet, Konstanz, 2010, S. 349–361.

Fuchs, Christian, Bundeswehr will soziale Netzwerke überwachen, Zeit Online vom 2.6.2014, http://www.zeit.de/politik/deutschland/2014-06/ueberwachung-bundeswehr-facebook-twitter-social-media (19.11.2015).

Fuchs, Martin, Social-Media-Instrumente im Schatten von Facebook und Twitter Best Practice-Beispiele aus deutschen Verwaltungen, in: Hill, Hermann (Hrsg.), E-Transformation, Veränderung der Verwaltung durch digitale Medien, Baden-Baden, 2014, S. 175–191.

Germann, Michael, Gefahrenabwehr und Strafverfolgung im Internet, Berlin, 2000.

Globig, Klaus/*Schuber*, Norbert/*Hartig*, Judith/*Klink*, Judith/*Eiermann*, Helmut (Hrsg.), Landesdatenschutzgesetz Rheinland-Pfalz (LDSG), Kommentar, Wiesbaden, 2009.

Gola, Peter/*Schomerus*, Rudolf (Hrsg.), BDSG, 12. Aufl., München, 2015.

Graf, Jürgen Peter (Hrsg.), Beck´scher Online- Kommentar StPO, 25. Ed., München, Stand: 2016.

Grün, Gianna-Carina, Terroristenjagd im sozialen Netz, Nach Worten wie "Flughafen" und "Terror" will die US-Heimatschutzbehörde bei Twitter, Facebook und anderen suchen. Was in Krisen hilft, finden Datenschützer unheimlich., Zeit Online vom 13.8.2011, http://www.zeit.de/digital/datenschutz/2011-08/monitoring-homeland-security (19.11.2015).

Hackenberg, Wolfgang, Teil 16.7 – Big Data, in: Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs, 43. Erg.-Lfg., München, 2016.

Henrichs, Axel/*Wilhelm*, Jörg, Polizeiliche Ermittlungen in sozialen Netzwerken, Kriminalistik 2010, S. 30–37.

Hill, Hermann, Staatskommunikation, JZ 1993, S. 330–336.

Hill, Hermann (Hrsg.), E-Transformation, Veränderung der Verwaltung durch digitale Medien, Baden-Baden, 2014.

Hill, Hermann/*Martini*, Mario/*Wagner*, Edgar (Hrsg.), Die digitale Lebenswelt gestalten, Baden-Baden, 2015.

Hoeren, Thomas/*Sieber*, Ulrich/*Holznagel*, Bernd (Hrsg.), Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs, 43. Erg.-Lfg., München, 2016.

Hoffmann, Christian/*Schulz*, Sönke E./*Borchers*, Kim Corinna, Grundrechtliche Wirkungsdimensionen im digitalen Raum, Bedrohungslagen im Internet und staatliche Reaktionsmöglichkeiten, MMR 2014, S. 89–95.

Hofmann, Olaf, Methoden des Social Media Monitoring, in: König, Christian/Stahl, Matthias/Wiegand, Erich (Hrsg.), Soziale Medien, Gegenstand und Instrument der Forschung, Wiesbaden, 2014, S. 161–170.

Hornung, G./*Müller-Terpitz*, R. (Hrsg.), Rechtshandbuch Social Media, 2015.

Hornung, Gerrit, Ein neues Grundrecht, Der verfassungsrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme, CR 2008, S. 299–306.

– , Datenschutzrechtliche Aspekte der Social Media, in: Hornung, G./Müller-Terpitz, R. (Hrsg.), Rechtshandbuch Social Media, 2015.

Jandt, Silke/*Roßnagel*, Alexander, Datenschutz in Social Networks - Kollektive Verantwortlichkeit für die Datenverarbeitung, ZD 2011, S. 160–166.

Jung, Alexander, Webrawling, Praxisrelevante Daten-Analyse im datenschutzrechtlichen Spannungsverhältnis, PinG 3 (2015), S. 170–174.

Karg, Moritz, Anmerkung zu EuGH: Löschungsanspruch gegen Google - "Recht auf Vergessen", ZD 2015, S. 359–361.

– Zugriff von Ermittlungsbehörden auf Nutzungsdaten bei der Strafverfolgung, Eine normierte Schutzlücke, DuD 2015, S. 85–88.

Kirchhof, Ferdinand, Zwischen Big Data und GG, AIB extra 2015, S. 6.

Klar, Manuel, Datenschutzrecht und die Visualisierung des öffentlichen Raums, Berlin, 2012.

Klär, Kerstin/*Tabino*, Oliver, Strategien und Methoden zur Behausung des Chaos – die Segmentierung des Social Web, in: Brauckmann, Patrick (Hrsg.), Web-Monitoring, Gewinnung und Analyse von Daten über das Kommunikationsverhalten im Internet, Konstanz, 2010, S. 235–263.

Klas, Benedikt, Grenzen der Erhebung und Speicherung allgemein zugänglicher Daten, Edewecht, 2012.

Koch, Frank A., Über die Unvereinbarkeit der deutschen und europäischen Datenschutzrechts mit Big Data, ITRB 2015, S. 13–20.

Kolonko, Petra, Punkte für Wohlverhalten, FAZ vom 7.5.2015, S. 5.

König, Christian/*Stahl*, Matthias/*Wiegand*, Erich (Hrsg.), Soziale Medien, Gegenstand und Instrument der Forschung, Wiesbaden, 2014.

Kudlich, Hans, Strafverfolgung im Internet, Bestandsaufnahme und aktuelle Probleme, GA 2011, S. 193–208.

Ladeur, Karl-Heinz (Hrsg.), Innovationsoffene Regulierung des Internet, Baden-Baden, 2003.

Leopold, Nils, Big Data – eine neue Herausforderung für den Datenschutz, Vorgänge 2012, S. 74–82.

Lobe, Adrian, Ist das ein Flüchtling oder ein Terrorist?, FAZ vom 17.2.2016, S. 13.

Lüge, Timo, Helfer ohne Grenzen, Wie Soziale Medien weltweit Hilfseinsätze verändern, Bevölkerungsschutz (3) 2014, S. 4–8.

Marthews, Alex/*Tucker*, Catherine, Government Surveillance and Internet Search Behavior, 29.4.2015, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2600645_code512675.pdf?abstractid=2412564&mirid=1 (26.11.2016).

Martini, Mario, Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl. 2014, S. 1481–1489.

– Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz, in: Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Die digitale Lebenswelt gestalten, Baden-Baden, 2015, S. 97–162.

– Do it yourself im Datenschutzrecht, Der „Geo Business Code of Conduct“ als Erprobungsfeld regulierter Selbstregulierung, NVwZ-Extra 3/2016, S. 1–13.

Martini, Mario/*Fritzsche*, Saskia, Kompendium Online-Bürgerbeteiligung, Rechtliche Rahmenbedingungen kommunaler Beteiligungsangebote im Internet, München, München, 2015.

– Mitverantwortung in sozialen Netzwerken, Fanpage-Betreiber in der datenschutzrechtlichen Grauzone, NVwZ-Extra 21/2015, S. 1–16.

Martini, Mario/*Weiß*, Wolfgang/*Ziekow*, Jan, Rechtliche Zulässigkeit flächendeckender Alarmierungen der Bevölkerung in Katastrophenfällen per SMS (KatWarn), Baden-Baden, 2013.

Masing, Johannes, Herausforderungen des Datenschutzes, NJW 2012, S. 2305–2311.

Maunz, Theodor/*Dürig*, Günter (Hrsg.), Grundgesetz, Loseblatt-Kommentar, 77. EGL, München, 2016.

Meinecke, Dirk, Big Data und Data Mining: Automatisierte Strafverfolgung als neue Wunderwaffe der Verbrechensbekämpfung?, in: Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht, 2014, S. 183–202.

Meyer, Alexander, Das Web 2.0 – Möglichkeiten und Grenzen der strafprozessualen Ermittlung in sozialen Netzwerken, Kriminalistik 2012, S. 759–764.

Möllers, Martin H.W./*Ooyen*, Robert Chr. (Hrsg.), Jahrbuch für öffentliche Sicherheit 2012/13, Frankfurt am Main, 2012.

Nettesheim, Martin, Grundrechtsschutz der Privatheit, VVDStRL 70 (2011), S. 7–49.

Nolte, Norbert, Das Recht auf Vergessenwerden – mehr als nur ein Hype?, NJW 2014, S. 2238–2242.

Oermann, Markus/*Staben*, Julian, Mittelbare Grundrechtseingriffe durch Abschreckung?, Zur grundrechtlichen Bewertung polizeilicher „Online-Streifen" und „Online-Ermittlungen" in sozialen Netzwerken, Der Staat 52 (2013), S. 630–661.

Orwell, George, Neunzehnhundertvierundachtzig, 21. Aufl., Zürich, 1973.

Penney, Jonathon W., Chilling Effects: Online Surveillance and Wikipedia Use, Berkeley Technology Law Journal 31 (2016), S. 117–182.

Petri, Thomas, Wertewandel am Datenschutz und die Grundrechte, DuD 2010, S. 25.

Plath, Kai-Uwe (Hrsg.), BDSG, Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG, Köln, 2013.

Plum, Alexander, Methoden und Technologien des Web-Monitorings – ein systematischer Vergleich, in: Brauckmann, Patrick (Hrsg.), Web-Monitoring, Gewinnung und Analyse von Daten über das Kommunikationsverhalten im Internet, Konstanz, 2010, S. 21–47.

Reißmann, Ole, Überwachung der Deutschen: So will die Regierung Facebook ausforschen, Spiegel Online vom 25.7.2014, http://www.spiegel.de/netzwelt/netzpolitik/weroq-regierung-erklaert-plaene-zur-facebook-ueberwachung-a-982846.html (19.11.2015).

Richter, Philipp, Die Wahl ist geheim… so what?, Big Data Mining im US-Wahlkampf. Und hier?, DÖV 2013, S. 961–970.

Roggan, Frederik, Die „Technikoffenheit" von strafprozessualen Ermittlungsbefugnissen und ihre Grenzen, NJW 2015, S. 1995–2000.

Schaar, Peter, Zwischen Big Data und Big Brother: zehn Jahre als Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, RDV 2013, S. 223–227.

Schild, Hans-Hermann/*Ronellenfitsch*, Michael/*Arlt*, Ute/*Dembowski*, Barbara, et al. (Hrsg.), Hessisches Datenschutzgesetz, Kommentar, 2016.

Schmid, Jan, Das neue Netz, Merkmale, Praktiken und Folgen des Web 2.0, 2. Aufl., München, 2011.

Schreiber, Marlene, Social Media Monitoring, PinG 2 (2014), S. 34–36.

Schulz, Sönke/*Hoffmann*, Christian, Staatliche Datenerhebung in sozialen Netzwerken, DuD 2012, S. 7–13.

– Soziale Medien in der öffentlichen Verwaltung, PdK - Band L 16 Bund, 2013.

Schulz, Sönke E., Einsatz von Social Media durch die öffentliche Verwaltung, in: Hornung, G./Müller-Terpitz, R. (Hrsg.), Rechtshandbuch Social Media, 2015.

Schulz, Sönke E./*Hoffmann*, Christian, Grundrechtsrelevanz staatlicher Beobachtungen im Internet, Internet-Streifen der Ermittlungsbehörden und das "Autorisierungskonzept" des BVerfG, CR 2010, S. 131–136.

Sen, Evrim, Social Media Monitoring für Unternehmen, Anforderungen an das Web-Monitoring verstehen & die richtigen Fragen stellen, Köln, 2011.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden, 2014.

Solmecke, Christian, Teil 21.1 - Social Media, in: Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs, 43. Erg.-Lfg., München, 2016.

Solmecke, Christian/*Wahlers*, Jakob, Rechtliche Situation von Social Media Monitoring-Diensten, ZD 2012, S. 550–555.

Spindler, Gerald/*Schuster*, Fabian (Hrsg.), Recht der elektronischen Medien, Kommentar, 3. Aufl., München, 2015.

Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht, 2014.

Taeger, Jürgen/*Gabel*, Detlev (Hrsg.), BDSG, 2. Aufl., Frankfurt am Main, 2013.

ULD Schleswig-Holstein, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, Kiel, 2014.

Ulmer, Claus-Dieter, BIG DATA - neue Geschäftsmodelle, neue Verantwortlichkeiten?, RDV 2013, S. 227–232.

Venzke-Caprese, Sven, Social Media Monitoring, Analyse und Profiling ohne klare Grenzen?, DuD 2013, S. 775–779.

Warntjen, Maximilian, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, Eine Konzeption im Anschluss an das Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung, BVerfGE 109, 279, Baden-Baden, Zürich, 2007.

Weber, Rolf H./*Thouvenin*, Florent (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich, 2014.

Weichert, Thilo, Facebook, der Datenschutz und die öffentliche Sicherheit, in: Möllers, Martin H.W./Ooyen, Robert Chr. (Hrsg.), Jahrbuch für öffentliche Sicherheit 2012/13, Frankfurt am Main, 2012, S. 379–391.

Weichert, Tilo, BDSG-Novelle zum Schutz von Internet-Inhaltsdaten, DuD 2009, S. 7–14.

Werner, Andreas, Social Media – Analytics & Monitoring, Verfahren und Werkzeuge zur Optimierung des ROI, Heidelberg, 2013.

Wolff, Heinrich Amadeus/*Brink*, Stefan (Hrsg.), Datenschutzrecht in Bund und Ländern, Grundlagen, bereichsspezifischer Datenschutz, BDSG, München, 2013.

Zerfaß, Ansgar/*Piwinger*, Manfred (Hrsg.), Handbuch Unternehmenskommunikation, Wiesbaden, 2007.

Zimmermann, Georg von, Die Einwilligung im Internet, Berlin, 2014.

Zisgen, Julia/*Kern*, Julia/*Voßschmidt*, Stefan, Aus Fremden werden Freunde, Deutsches Recht und Soziale Medien, Bevölkerungsschutz (3) 2014, S. 9–13.