Ausarbeitung

Social Media und Datenschutz

Social Media und Datenschutz

Aktenzeichen: WD 3 - 3000 - 023/20
Abschluss der Arbeit: 7. Februar 2020
Fachbereich: WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Einleitung

Es wurde erbeten, die rechtliche Diskussion zum Thema „Social Media und Datenschutz“ darzustellen. Dabei steht die Möglichkeit der Nutzung der Portale Twitter und YouTube durch Behörden oder Verfassungsorgane im Mittelpunkt. Im Folgenden wird auf die wesentlichen datenschutzrechtlichen Probleme eingegangen. Weder in der Rechtsprechung noch in der Literatur wurde bisher eine detaillierte Prüfung der gesamten Datenverarbeitungsvorgänge von Social-Media-Auftritten auf Twitter oder YouTube vorgenommen. Allerdings liegen zwei Entscheidungen des Europäischen Gerichtshofs und des Bundesverwaltungsgerichts vor, die eine gemeinsame datenschutzrechtliche Verantwortlichkeit von Fanpagebetreibern und den Betreibern von Facebook annehmen. Auf welche weiteren Angebote in sozialen Netzwerken diese Rechtsprechung übertragbar ist und welche datenschutzrechtliche Bewertung sich daraus für Social-Media-Auftritte von öffentlichen Stellen ergeben, ist bislang nicht abschließend geklärt und wird derzeit in Fachkreisen diskutiert. Einige Landesdatenschutzbeauftragte empfehlen Behörden, sich aus sozialen Medien, insbesondere von Twitter zurückzuziehen.[1] Der Landesbeauftragte Baden-Württembergs für Datenschutz und Informationsfreiheit (LfDI), Herr Dr. Stefan Brink, hat nun als erste deutsche Aufsichtsbehörde eine an das aktuell geltende Datenschutzrecht angepasste Richtlinie zur Nutzung von sozialen Netzwerken durch öffentliche Stellen veröffentlicht. Ferner werden die in der Literatur und durch Aufsichtsbehörden auf europäischer und Bundesebene geäußerten Positionen in die Darstellung einbezogen. Ergebnisse einer laufenden Prüfung des Bundesministeriums der Justiz und für Verbraucherschutz und des Bundespresseamtes liegen noch nicht vor.[2]

2. Vorbemerkung

Vorab ist darauf hinzuweisen, dass für die Festlegung des jeweils geltenden Rechtsmaßstabes maßgeblich ist, ob ein **personalisierter Account** einen **behördlichen** oder **privaten Charakter** hat, so zum Beispiel der Account von Regierungsmitgliedern oder dem Bundestagspräsidenten.[3]

Relevant ist auch, welchen **Zwecken** ein Social-Media-Auftritt dient. Grundsätzlich kommen für die Social-Media-Nutzung durch Behörden folgende Zwecke in Betracht:

– „Passive” Informationsbeschaffung (Social Media als Quelle für die Recherche und Informationen)

---

1 So etwa der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (näher unter 3.4.), die Berliner Beauftragte für Datenschutz und Informationsfreiheit (vgl. Der Tagesspiegel vom 11. Januar 2020, S. 7, Behörden sollen raus aus Twitter) und der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (vgl. Westdeutsche Zeitung vom 9. Januar 2020, Warum Behörden nicht twittern sollten, abrufbar unter: https://www.wz.de/nrw/nrw-datenschuetzerin-raet-behoerden-von-twitter-ab_aid-48239669 (zuletzt abgerufen am: 7.2.2020)

2 Der Tagesspiegel vom 7. Februar 2020, Ausgezwitschert und Abgeschaltet, S. 7.

3 Zur Bedeutung des Impressums eines Accounts für diese Abgrenzungsfrage und einer Zweifelsregelung zur Annahme einer behördlichen Rolle: Harding, Die Charakterisierung staatlicher Accounts in sozialen Netzwerken, NJW 2019, 1910 ff.; Hinsichtlich des Bundestagspräsidenten müsste zusätzlich unterschieden werden, ob er als solcher oder als Mitglied des Deutschen Bundestages den Account betreibt.

- Presse- und Öffentlichkeitsarbeit (Möglichkeit, schnell den gewünschten Adressatenkreis zu erreichen und von diesem möglichst umfassend wahrgenommen werden)
- Bürgerkommunikation (direkte Kommunikation mit Bürgerinnen und Bürgern, etwa zur Beantwortung von Bürgeranfragen oder für das Beschwerdemanagement)
- „Aktive" Informationsbeschaffung (direkte Aufforderung zur Information)
- Fachlicher Diskurs (direkter Austausch mit anderen Fachleuten oder Interessierten über Wissen und Meinungen)
- Kommunikation im Intranet (zur internen Organisation von Arbeitsprozessen).[4]

Diese Ausarbeitung konzentriert sich auf das Ziel der Nutzung sozialer Medien zur **Öffentlichkeitsarbeit**. Soweit die Dienste auch auf die Kommunikation mit den Nutzern gerichtet sind, entstehen noch mehr Berührungspunkte zu sensiblen Daten. Messengerdienste erfordern eine gesonderte Betrachtung.

Eine Erhebung der Wissenschaftlichen Dienste hat Anfang des Jahres 2019 ergeben, dass die **Parlamente** der neun größten **EU-Mitgliedstaaten** weit überwiegend über einen Facebook-, Twitter-, Instagram- und YouTube-Account verfügen.[5] Das Europäische Parlament verfügt neben diese Accounts auch noch über solche bei Flickr, LinkedIn, Pinterest, Snapchat, Reddit und Google+.

3. Datenschutzrecht

Sofern die Datenverarbeitung durch öffentliche Stellen, wie etwa durch Polizeibehörden, nicht der EU-Datenschutzrichtlinie für Justiz und Inneres[6] (JI-Richtlinie) unterfällt,[7] ist die Datenschutzgrundverordnung[8] (DSGVO) auf **öffentliche Stellen** des Bundes entweder direkt oder gemäß § 1

---

4 Nach Niedersachsen, Bekanntmachung: Umgang mit webbasierten sozialen Medien (Social Media) (Bek. d. MI v. 18.10.2012 – 42.02840/1100-0003, Nds. MBl. S. 885), Anlage zum Behörden-Leitfaden: Umgang mit webbasierten sozialen Medien (Social Media).

5 Wissenschaftliche Dienste des Deutschen Bundestages, Europäische Parlamente im Bereich Social Media, WD 10 - 3000 - 013/19 vom 31.01.2019.

6 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4. Mai 2016, S. 89.

7 Die JI-Richtlinie gilt nach Art. 1 i.V.m. Art. 2 Abs. 1 für die Datenverarbeitung durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

8 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4. Mai 2016, S. 1.

Abs. 8 BDSG jedenfalls entsprechend anwendbar. Das VG Wiesbaden hat den Europäischen Gerichtshof im März 2019 um Vorabentscheidung über die grundsätzliche Frage ersucht, ob und inwieweit die DSGVO auch für **nationale Parlamente** unmittelbar gilt.[9] Anders als das Bundesrecht sieht das hessische Landesdatenschutzrecht ausdrücklich Ausnahmen für das Parlament vor, soweit es nicht in Verwaltungsangelegenheiten tätig wird und überlässt die ausgenommenen Bereiche der Regelung des Parlaments durch eine eigene Datenschutzordnung. Eine Entscheidung des Europäischen Gerichtshofs liegt noch nicht vor.

Für den Bundestag führt die schwierige Abgrenzung der Datenverarbeitung zur Wahrnehmung parlamentarischer Aufgaben von Verwaltungstätigkeiten des Parlaments wegen der Anordnung der entsprechenden Geltung der DSGVO in § 1 Abs. 8 BDSG nicht zu unterschiedlichen datenschutzrechtlichen Vorgaben.

Das Datenschutzrecht schützt alle personenbezogenen Daten. Diese werden in Art. 4 Nr. 1 DSGVO wie folgt legaldefiniert:

> *„**‘personenbezogene Daten‘** [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person‘) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.*

Demnach gibt es in Bezug auf Personen auch **kein belangloses Datum**.

Für die Anwendung des Datenschutzrechts muss ein personenbezogenes Datum verarbeitet werden. Art. 4 Nr. 1 DSGVO definiert:

> *„**‘Verarbeitung‘** [als] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“*

Datenschutzrechtliche Einschränkungen können sich insofern einerseits für die **Einrichtung von Accounts** in sozialen Netzwerken ergeben, davon unabhängig aber auch bezüglich der **Nutzung** und potentieller **Inhalte** von Tweets, Nachrichten, Posts, Bildern oder Videos, die in den Netzwerken verbreitet werden, soweit diese sich auf personenbezogene Daten beziehen.

---

9 VG Wiesbaden, Beschluss vom 28.3.2019, Az. 6 K 1016/15.Wi, juris; das Vorabentscheidungsverfahren vor dem Europäischen Gerichtshof wird unter dem Az. C-272/19 geführt.

3.1. Rechtsprechung des Bundesverwaltungsgerichts und des Europäischen Gerichtshofs zur datenschutzrechtlichen Verantwortlichkeit beim Betreiben von Fanpages in sozialen Medien

Das Bundesverwaltungsgericht hat den Europäischen Gerichtshof in einem **Vorabentscheidungsverfahren** um Auslegung mehrerer Bestimmungen der Datenschutzrichtlinie im Zusammenhang mit dem Betrieb von Fanpages in sozialen Netzwerken gebeten. Fanpages sind Benutzerkonten von Privatpersonen oder Unternehmen, die dazu dienen, sich sowohl den Nutzern dieses sozialen Netzwerks als auch externen Besuchern zu präsentieren und Äußerungen aller Art in den Medien- und Meinungsmarkt einzubringen. Der Europäische Gerichtshof hatte vor allem darüber zu urteilen, ob auch der Betreiber einer Facebook-Fanpage als bloßer Nutzer neben den Betreibern der Plattform Verantwortlicher für die Datenschutzverarbeitung im Sinne der Datenschutz-Richtlinie (Datenschutz-RL) ist. Die Datenschutz-RL wurde durch die heute geltende DSGVO abgelöst, die den hier entscheidenden Punkten der alten Regelungslage aber weitgehend entspricht.

3.1.1. Europäischer Gerichtshof (Große Kammer), Urteil vom 5.6.2018 – C-210/16

Der Europäische Gerichtshof urteilte, dass in erster Linie der **Plattformbetreiber** selbst, in dem Falle Facebook, „für die Verarbeitung Verantwortlicher“ im Sinne der Datenschutz-RL ist. Zudem ist auch der Betreiber einer Fanpage für diese **Verarbeitung verantwortlich**. Zur Begründung führt der Europäische Gerichtshof aus, dass die Datenverarbeitung zwar in erster Linie durch Facebook, etwa durch **Platzierung von Cookies** auf den IT-Geräten der Besucher, erfolge; allerdings erhalte Facebook diese Möglichkeit erst durch Einrichtung einer solchen Fanpage seitens des Betreibers, im Rahmen dessen dieser den Nutzungsbedingungen, wie auch den entsprechenden Cookie-Richtlinien zustimmte. Erst so ergebe sich die Möglichkeit für Facebook, Cookies zu platzieren und zwar unabhängig davon, ob die Person über ein Facebook-Konto verfügt. Überdies dienten die Daten nicht lediglich Facebook selbst, sondern sollen auch dem **Betreiber** ermöglichen, die **Vermarktung seiner Tätigkeit** zu steuern. Die Betreiber können spezifische von Facebook aufgrund der Seitenbesuche erstellte Besucherstatistiken – wie etwa demografische oder geografische Daten – einsehen und ihr Angebot dadurch zielgerichtet gestalten. Die Kriterien, nach denen diese Statistiken erstellt werden, und sogar die Kategorien von Personen, deren personenbezogene Daten von Facebook ausgewertet werden sollen, kann der Betreiber durch Filter festlegen. So wirkt er unmittelbar auf die Datenauswertung durch Facebook ein. Zwar werden die Statistiken ausschließlich in anonymisierter Form an den Betreiber übermittelt, beruhen jedoch auf der personenbezogenen Datenerhebung durch Facebook.

Zudem stellte der Europäische Gerichtshof fest, dass die Anwendbarkeit deutschen Datenschutzrechts auf die bei Aufruf der Fanpage durch Facebook vorgenommene Datenverarbeitung gegeben ist. Verstöße können nicht nur gegenüber der Fanpageseitenbetreiberin, sondern auch gegenüber den in Europa ansässigen, an der Datenverarbeitung auch beteiligten Niederlassungen von Facebook geltend gemacht werden.

3.1.2. Bundesverwaltungsgericht, Urteil vom 11.9.2019 – 6 C 15/18

Im Anschluss an das Urteil des Europäischen Gerichtshofs wurde das Revisionsverfahren vor dem Bundesverwaltungsgericht fortgesetzt. Die Datenschutz-RL wurde zum damaligen Zeitpunkt durch das – inzwischen an die DSGVO angepasste – Bundesdatenschutzgesetz (BDSG) umgesetzt. Das Bundesverwaltungsgericht musste insofern auch für das deutsche Recht die Frage nach der datenschutzrechtlichen Verantwortlichkeit der Akteure klären. Es entschied unter Zugrundelegung des

Urteils des Europäischen Gerichtshofs, dass die Betreiberin der Fanpage auch nach dem BDSG datenschutzrechtlich verantwortlich ist. Der Begriff der verantwortlichen Stelle i.S.v. § 3 Abs. 7 BDSG a.F. sei unionsrechtskonform dahingehend zu verstehen, dass er auch Stellen erfasst, die anderen die Gelegenheit der Datenverarbeitung einräumen, ohne selbst damit befasst zu sein. Auch durfte die Fanpagebetreiberin anstelle des Facebook-Konzerns als Adressatin der datenschutzrechtlichen Verfügung zur Abstellung der rechtswidrigen Handlung herangezogen werden. Auch im Bereich des Datenschutzes könne das Gebot einer effektiven und wirkungsvollen Gefahrenabwehr es rechtfertigen, denjenigen Verantwortlichen heranzuziehen, dessen Pflichtigkeit sich ohne weiteres bejahen lasse und dem **effektive Mittel zum Abstellen des Verstoßes** zur Verfügung stünden. Zudem erweise sich die Anordnung gegen die Klägerin auch als effektives Mittel, das von der Datenschutzrichtlinie bezweckte **hohe Datenschutzniveau** zu gewährleisten, da die Anordnung, geeignet sei, Facebook Ireland über den Einzelfall der Klägerin hinaus unter Zugzwang zu setzen, sich um eine datenschutzkonforme Lösung zu bemühen. Das Bundesverwaltungsgericht hob das Berufungsurteil auf und verwies den Rechtsstreit an das schleswig-holsteinische Oberverwaltungsgericht zurück.

3.1.3. Praxisfolgen insbesondere im Hinblick auf Rechtslage nach Inkrafttreten der DSGVO

Zunächst ist festzuhalten, dass die Entscheidung **keine Aussage** darüber trifft, ob und inwieweit die Datenverarbeitung durch Facebook **datenschutzwidrig** erfolgt. Diese Prüfung obliegt nun dem zuständigen Oberverwaltungsgericht als Tatsacheninstanz.

Im Hinblick auf die nunmehr geltende DSGVO ist festzustellen, dass die entscheidende Begriffsbestimmung aus Art. 2 d) der Datenschutz-RL im Kern in Art. 4 Nr. 7 und Art. 26 DSGVO übernommen wurden. Dies indiziert, dass das Urteil des Europäischen Gerichtshofs bezüglich der Frage der Verantwortlichkeit auch im Anwendungsbereich der DSGVO Bestand haben wird. Darüber hinaus haben Betreiber von Fanpages nunmehr Art. 26 DSGVO zu berücksichtigen, der sicherstellen soll, dass alle Verantwortlichen für eine transparente Verarbeitung und die Wahrung der Betroffenenrechte sorgen. Als erste Reaktion auf das Urteil des Europäischen Gerichtshofs haben die Datenschutzaufsichtsbehörden des Bundes und der Länder im Rahmen der Datenschutzkonferenz[10] auf folgende Pflichten der Betreiber von Fanpages hingewiesen: Entschließen sich Unternehmen oder Behörden zur Errichtung einer Fanseite auf der Plattform Facebook, sind auch sie verpflichtet, im Rahmen von Vereinbarungen mit Facebook für eine **transparente Verarbeitung** zu sorgen. Diese Vereinbarung muss den Betroffenen in wesentlichen Punkten zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können. Es gilt sicherzustellen, dass die Besucher der Fanpages – registrierte wie auch nicht registrierte – in verständlicher Form über die Datenverarbeitung informiert werden. Die Unternehmen selbst müssen sich versichern, dass Facebook ihnen die Informationen zur Einhaltung dieser Pflichten zur Verfügung stellt. Zu beachten ist zudem, dass bei **Daten-Tracking** seitens Facebook (etwa durch Einsatz von Cookies etc.), nach Einschätzung der Datenschutzaufsichtsbehörden grundsätzlich eine **Einwilligung** der Nutzenden erforderlich ist, die zumindest die Anforderungen der Art. 4 Nr. 11, Art. 7 und 8

10 Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) vom 6.6.2018, Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/20180605_en_fb_fanpages.pdf (zuletzt aufgerufen am 5.2.2020).

DSGVO erfüllt. Dabei muss insbesondere beachtet werden, dass das Informationsangebot auch von Personen genutzt werden kann, die nicht über ein Facebook-Konto verfügen.

Sowohl der Bundesbeauftragte für Datenschutz und Informationsfreiheit[11] (BfDI) als auch der LfDI Baden-Württemberg[12] halten die Entscheidung des Europäischen Gerichtshofs und des Bundesverwaltungsgerichts auf **weitere Social-Media-Angebote für übertragbar** und nach Prüfung der Datenschutzbestimmungen der Anbieter eine gemeinsame Verantwortung nach Art. 26 DSGVO für möglich.[13]

3.2. Anwendbares Datenschutzrecht für Social-Media-Auftritte öffentlicher Stellen

Datenschutzrechtlich ist bei Social-Media-Auftritten im Rahmen der Öffentlichkeitsarbeit von öffentlichen Stellen zwischen den auf diesen Kanälen **veröffentlichten Inhalten** (insb. Bildaufnahmen und sonstige personenbezogene Daten) und den **sonstigen Datenverarbeitungsvorgängen** im Rahmen von Tools zur Personalisierung der einzelnen Nutzern angezeigten Inhalte und ggf. **Werbung** und der Erstellung von **Nutzerstatistiken** und **Auswertung** von **Nutzerverhalten** zu unterscheiden. Die nachfolgenden Ausführungen sind nicht auf zusätzliche Kommentar- und Direktnachrichtenfunktionen von Social-Media-Plattformen oder auf die Bereitstellung öffentlicher Leistungen über Internetseiten bezogen.

Art. 85 Abs. 1 DSGVO, der eine **Regelungsbefugnis** für nationales Datenschutzrecht enthält, wenn die Zwecke der Datenverarbeitung der freien Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken dienen, ist auf öffentliche Stellen nicht anwendbar. Die Regelung soll gerade die Grundrechte der Meinungs-, Informations- und Pressefreiheit schützen, auf die der Staat selber sich nicht berufen kann.

Mithin richtet sich die Zulässigkeit der Datenverarbeitung nach der zentralen Regelung des **Art. 6 Abs. 1 DSGVO**. Danach ist die Datenverarbeitung nur dann rechtmäßig, wenn mindestens einer der in lit. a) bis f) genannten Erlaubnistatbestände erfüllt ist.

In Art. 6 Abs. 1 S. 1 **lit. a)** DSGVO ist geregelt, dass die Datenverarbeitung dann erfolgen kann, wenn eine **Einwilligung** der betroffenen Person zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke erfolgt ist. Die Einwilligung muss nach Art. 4 Nr. 11 DSGVO freiwillig und in informierter Weise und unmissverständlich sowie durch Erklärung oder eine sonstige eindeutige bestätigende Handlung erfolgen.

Nach einer Meinung könnten sich Behörden nur sehr eingeschränkt auf eine Einwilligung berufen, da die Freiwilligkeit für die Wirksamkeit der Einwilligung dann in Frage stehe, wenn die Behörde

---

11 Dazu näher unter 3.5. und 3.6., vgl. auch Unterrichtung durch den BfDI, Tätigkeitsbericht 2017 und 2018 zum Datenschutz (27. Tätigkeitsbericht), BT-Drs. 19/9800, S. 110 ff.

12 Dazu näher unter 3.4.

13 Mit a.A. zu Definition des EuGH anhand weiterer Kriterien differenzierend Kremer, Gemeinsame Verantwortlichkeit: Die neue Auftragsdatenverarbeitung?, CR 2019, 225, 233.

die Zustimmung im Zweifel auch erzwingen könnte.[14] Da es bei Social-Media-Auftritten aber nicht um eine erzwingbare staatliche Datenverarbeitung geht, sondern in erster Linie um die **Öffentlichkeitsarbeit**, kann insofern auf weitere Abgrenzung verzichtet werden und eine Einwilligung in die Datenverarbeitung scheint grundsätzlich möglich. Nach Art. 7 Abs. 4 DSGVO kann es aber an der Freiwilligkeit der Einwilligung fehlen, wenn die Erfüllung eines Vertrags bspw. zwischen Betreibern von Social-Media-Angeboten und ihren Nutzern, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind (sog. Koppelungsverbot). Probleme könnten sich insbesondere hinsichtlich der Einwilligung in personalisierte Werbung oder in umfassende Datensammlungen auch über Drittquellen und die Zusammenführung der Daten[15] ergeben, wenn diese in unzulässiger Weise mit anderen Einwilligungen gekoppelt wird.

Neben Art. 6 Abs. 1 S. 1 lit. a) kommt auch **lit. e)** DSGVO als Rechtsgrundlage in Betracht. Danach ist die Datenverarbeitung zulässig, wenn sie für die Wahrnehmung einer **Aufgabe** erforderlich ist, die im **öffentlichen Interesse** liegt oder in **Ausübung öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde. Eine gesetzliche Regelung, die die Datenverarbeitung zum Zwecke der Öffentlichkeitsarbeit von Behörden erlaubt, existiert auf Bundesebene nicht. Öffentlichkeitsarbeit durch Behörden innerhalb des eigenen Aufgaben- und Zuständigkeitsbereiches ist als öffentliche Aufgabe aber anerkannt und durch das Bundesverfassungsgericht bestätigt worden.[16] Insofern kommt Art. 6 Abs. 1 S. 1 **lit. e)** DSGVO i.V.m. der Generalklausel des § 3 BDSG als Rechtsgrundlage für die Verarbeitung personenbezogener Daten für Social-Media-Auftritte von öffentlichen Stellen in Betracht. Die Datenverarbeitung muss jedoch im Einzelfall hinsichtlich Art und Umfang auch **erforderlich** sein. Problematisch könnte beispielsweise die Auswertung der Nutzerdaten zur Erstellung von Nutzungsprofilen oder Nutzerstatistiken oder zur Personalisierung von Inhalten und Werbung sein. Teilweise bieten Social-Media-Plattformen auch die Möglichkeit, die Datenverarbeitung einzuschränken.

Die **Personalisierung von Inhalten** des Social-Media-Auftritts kann grundsätzlich zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen nach Art. 6 Abs. 1 S. 1 **lit. b)** DSGVO gerechtfertigt sein.[17]

Die Datenverarbeitung durch nicht-öffentliche Stellen zum Zwecke der Anzeige **personalisierter Werbung** kann nach überwiegender Ansicht durch eine Einwilligung nach Art. 6 Abs.1 S. 1 lit. a)

---

14 Kühling/Buchner, in: Buchner/Petri (Hrsg.), 2. Aufl. 2018, DS-GVO Art. 6, Rn. 22.

15 Bundeskartellamt, Konditionenmissbrauch gem. § 19 I GWB wegen unangemessener Datenverarbeitung, Entscheidung v. 6.2.2019 – B6-22/16, Fallbericht v. 15.2.2019, abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf;jsessionid=3C7191EAEBF55B802EF54F6DA4D5C054.1_cid378?__blob=publicationFile&v=3 (zuletzt aufgerufen am 6.2.2020).

16 BVerfGE 44, 125, 147 ff.; BVerfGE 63, 230, 242 ff.

17 Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0, 8. Oktober 2019, Pkt. 3.4 S. 15, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf (zuletzt aufgerufen am 6.2.2020).

DSGVO oder aber zur Wahrnehmung berechtigter Interessen des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 S. 1 lit. f) DSGVO gerechtfertigt sein.[18] Art. 6 Abs. 1 S. 1 lit. f) ist jedoch gemäß Abs. 1 S. 2 DSGVO ausdrücklich nicht für Behörden anwendbar. Insofern kommt diese Norm ebenso wenig wie Art. 6 Abs. 1 S. 1 **lit. b)**[19] als Rechtfertigung für die Datenverarbeitung durch öffentliche Stellen in Betracht.

Ferner gelten besondere Anforderungen an die **Datenübermittlung** an verarbeitende Stellen in **Drittländern.**[20] Diese Vorgaben spielen bei Social-Media-Auftritten eine besondere Rolle, da deren Betreiber ihren Sitz häufig im EU-Ausland haben.

Sofern die Inhaber von Social-Media-Auftritten mit den Plattformbetreibern **gemeinsam** für die **Datenverarbeitung verantwortlich** sind,[21] müssen diese gemäß **Art. 26 DSGVO** und **§ 63 BDSG** in einer **Vereinbarung** in transparenter Form festlegen, wer von ihnen welche Verpflichtung nach der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Art. 13 und 14 DSGVO nachkommt, sofern und soweit dies nicht bereits durch Unions- oder nationales Recht geregelt ist. Der LfDI Baden-Württemberg wies darauf hin, dass Behörden ihren Account löschen und auf andere Anbieter ausweichen müssten, wenn ein Betreiber wie Twitter nicht bereit sei, einen Nutzungsvertrag zu unterschreiben.[22]

Ist die Nutzung von personenbezogenen Daten grundsätzlich auf Grundlage eines Erlaubnistatbestandes zulässig, gelten für deren Verarbeitung die weiteren **datenschutzrechtlichen Anforderungen**, wie die einer hinreichenden **Transparenz**, der **Datensparsamkeit**, etc., aber ggf. auch weitere Vorgaben, so zum Beispiel bei der Verwendung von Bildern die des **Kunsturhebergesetzes**.[23]

3.3. Weitere datenschutzrechtliche Bestimmungen

Zu beachten ist auch, dass sich das Datenschutzrecht bezüglich Social Media zukünftig noch weiter verschärft. Der – seit drei Jahren diskutierte, aber seit Ende 2019 noch einmal in grundlegender

---

18 DSK, Kurzpapier Nr. 3 Verarbeitung personenbezogener Daten für Werbung, Stand 17. 12. 2018, S. 1, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_3.pdf (zuletzt aufgerufen am 6.2.2020).

19 Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0, 8. Oktober 2019, Pkt. 3.3 S. 14, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf (zuletzt aufgerufen am 6.2.2020).

20 DSK, Kurzpapier Nr. 4, Datenübermittlung in Drittländer, stand: 22.7.2019, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf (zuletzt aufgerufen am 6.2.2020).

21 Kremer, Gemeinsame Verantwortlichkeit: Die neue Auftragsdatenverarbeitung?, CR 2019, 225, 233.

22 Frankfurter Allgemeine vom 29. Januar 2020, Rechtswidrige Tweets? Dürfen Behörden noch auf sozialen Medien präsent sein?, S. 6.

23 Krüger/Wiencke, Bitte recht freundlich – Verhältnis zwischen KUG und DS-GVO, MMR 2019, 76 ff.

Überarbeitung befindliche – Entwurf der **ePrivacy-Verordnung**[24] wird auf die sozialen Medien erheblichen Einfluss haben. Nach der Verordnung sollen unter anderem Datensammlungen im Internet über Cookies beschränkt werden.

Darüber hinaus ist beim Betrieb von Social-Media-Accounts auch durch öffentliche Stellen das **Telemediengesetz** (TMG) zu beachten.[25] Dieses wurde bislang allerdings noch nicht an die DSGVO angepasst. Die DSGVO ist daher insbesondere gegenüber den datenschutzrechtlichen Vorschriften des Kapitels 4 des TMG vorrangig anzuwenden.[26]

Bedeutung kommt ebenfalls dem **Ort** der **Datenverarbeitung** und Speicherung zu.[27] Wenn dieser in Nicht-EU-Staaten liegt, so ist bezüglich des Datenschutzes ein **Angemessenheitsbeschluss** der EU-Kommission erforderlich, der aussagt, dass vom Drittland ein der EU vergleichbares Datenschutzniveau im Umgang mit personenbezogenen Daten aus der EU gewährleistet wird (Art. 45 Abs. 3 DSGVO). Als Angemessenheitsbeschluss gilt das **EU-US-Privacy Shield** aus 2016 für die datenverarbeitenden Unternehmen in den USA, die speziell gelistet sind. Dies ist bei den Betreibern der sozialen Netzwerke in der Regel der Fall. Jedoch ist zu beachten, dass das EU-US-Privacy Shield seit Inkrafttreten der DSGVO erneut hinterfragt wird und unter anderem das Europäische Parlament eine Überprüfung verlangt.[28] Anlass dafür war unter anderem der Datenskandal um Facebook und Cambridge Analytica. Auch die Bedeutung des US-amerikanischen CLOUD Acts könnte insoweit Relevanz entfalten.[29]

3.4. Bewertung des Landesbeauftragen für Datenschutz Baden-Württemberg

Der **LfDI Baden-Württemberg** Dr. Stefan Brink löschte mit Verweis auf datenschutzrechtliche Bedenken nach der oben ausgeführten Entscheidung des Bundesverwaltungsgerichts seinen **Twitter**-Account Anfang 2020. Er machte deutlich, dass er auch eine datenschutzrechtliche gemeinsame Verantwortlichkeit zwischen Seitenbetreiber und Netzwerkbetreiber bei Twitter sehe

---

24 Vorschlag der EU-Kommission abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52017PC0010 (zuletzt aufgerufen am 6.2.2020).

25 Zum Datenschutz bei der Telemediennutzung durch nicht-öffentliche Stellen DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand: März 2019, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf (zuletzt aufgerufen am 6.2.2020).

26 DSK, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Stand: 26. April 2018, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/201804_ah_positionsbestimmung_tmg.pdf (zuletzt aufgerufen am 6.2.2020).

27 Für nicht geklärt hält auch der LfDI Baden-Württembergs grundlegende Rechtsfragen im Falle der außereuropäischer Plattformbetreiber/-anbieter, LfDI Baden-Württemberg, Wesentliche Anforderungen an die behördliche Nutzung „Sozialer Netzwerke“, 6.2.2020, siehe Anlage 1.

28 Entschließung des Europäischen Parlaments zur Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (2018/2645(RSP)), vom 26.6.2018 insbesondere Nr. 31 bis 35, abrufbar unter: http://www.europarl.europa.eu/doceo/document/B-8-2018-0305_DE.html (zuletzt aufgerufen am 5.2.2020).

29 Dazu näher: Wissenschaftliche Dienste des Deutschen Bundestages, Datenübermittlung an US-Ermittlungsbehörden auf Grundlage des CLOUD Acts im Geltungsbereich des EU-Datenschutzrechts, WD 3 - 3000 - 205/19 vom 20. August 2019.

und Twitter ebenfalls im Hintergrund Daten der Nutzer sammle. Dies halte er auch für andere Behörden für geboten.[30] Er argumentiert insoweit auch mit der rechtsstaatlich begründeten Vorbildfunktion.

Am 6. Februar 2020 hat der LfDI einen Leitfaden mit den wesentlichen Anforderungen an die behördliche Nutzung „Sozialer Netzwerke“ veröffentlicht.

Anlage 1

Nach seiner Prüfung sind demnach vor allem folgende Anforderungen einzuhalten:

1. Behördliche Mitglieder müssen eine **datenschutzrechtliche Rechtsgrundlage** vorweisen können (insbesondere eine Einwilligung des Betroffenen, oder bei nicht nur reiner Öffentlichkeitsarbeit – z.B. zum Schutz der öffentlichen Sicherheit bei der Warnung vor Umweltkatastrophen – Art. 6 Abs. 1 S. 1 lit. f) DSGVO i.V.m. einer fachgesetzlichen Regelung; für empfehlenswert hält er ein Gesetz für die Öffentlichkeitsarbeit von Behörden).

2. Die datenschutzrechtlichen **Transparenzgebote** müssen eingehalten werden, nach der jegliche Verarbeitung personenbezogener Daten offengelegt werden muss.

3. Soweit behördliche Mitglieder mit dem Plattformbetreiber zusammen **gemeinsam verantwortlich** für **Datenverarbeitungen** sind, muss dazu eine **vertragliche Vereinbarung** getroffen werden. In dieser soll klar verteilt werden, wer für die Einhaltung welcher Verpflichtungen der DSGVO verantwortlich ist, was auch eine vollständige Offenlegung sämtlicher Verarbeitungen personenbezogener Daten verlangt.

4. Zudem sei eine **kontinuierliche redaktionelle Betreuung** des eigenen Angebots erforderlich und es seien die Pflichten aus dem Telemediengesetz zu erfüllen, insbesondere auch hinsichtlich des Umgangs mit rechtswidrigen Posts Dritter auf der eigenen Seite.

5. Behördliche Mitglieder müssen **alternative Informations- und Kommunikationswege** anbieten, damit Bürgerinnen und Bürger nicht in „Soziale Netzwerke“ hineingezwungen werden.

6. Die technischen und organisatorischen **Sicherungsmaßnahmen** müssen dem Stand der Technik genügen und der **Selbstschutz** der Bürgerinnen und Bürger muss respektiert werden, z.B. deren Einstellungen zu Cookies oder die Deaktivierung der Standortdaten.

3.5. Twitter

Der BfDI hat gegenüber dem Bundestag eine knappe Bewertung der Einsatzmöglichkeiten von Twitter vorgenommen. Nach seiner Einschätzung sei der Einsatz von Twitter möglich, soweit

30 Handelsblatt online vom 1.1.2020, Datenschützer rät Behörden und Firmen zur Abkehr von Twitter, abrufbar unter: https://www.handelsblatt.com/politik/deutschland/stefan-brink-datenschuetzer-raet-behoerden-und-firmen-zur-abkehr-von-twitter/25381124.html?ticket=ST-2646727-BRDAQVk69x9LQRQtvzrG-ap2 (zuletzt aufgerufen am 6.2.2020).

bestimmte datenschutzfreundliche Einstellungen vorgenommen würden. Dazu zähle die dauerhafte Deaktivierung des Dashboards und keine Nutzung der Direktnachrichtenfunktion, weil diese die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO verhindere. Die Nutzung von Twitter solle in ein Social-Media-Konzept eingebettet sein, nach dem Informationen nicht exklusiv auf Twitter geteilt werden sollen. Plugins oder Links sollten nur so eingebettet werden, dass bei Aufruf der Seite noch keine Daten übertragen werden.

Auch Ingold[31] trug 2017 besondere Bedenken gegenüber der Datenschutzrechtskonformität der Twitter-Nutzung vor. Vor allem die **Datenherrschaft** sei bei Twitter auch nach Löschung oder Korrektur einzelner Tweets erschwert, da Tweets durch die Möglichkeit der Vervielfältigung von Beiträgen (Retweets) präsent bleiben können. Twitter strebe aber, wofür auch die Möglichkeit der Nutzung von **Pseudonymen** als Profilnamen spreche, keine (zu Facebook vergleichbare) umfassende Auswertung der Nutzer- und Inhaltsdaten an. Er schlägt zur Behebung von datenschutzrechtlichen Problemen bezüglich selbst geteilter personenbezogener Daten vor, dass über die Einbindung von Links oder sog. Inline-frame-Lösungen, bei denen über eine HTML-Element Inhalte der staatlichen Website dynamisch in den Social-Media-Kanal eingebettet werden, die Datenherrschaft erhalten bleibt und externe Auswertungen erschwert werden. Im Ergebnis hält Ingold also eine datenschutzkonforme Nutzung von Twitter für möglich.

3.6. YouTube

Der BfDI wies in seiner Stellungnahme gegenüber dem behördlichen Datenschutzbeauftragten des Bundestages im Juni 2019 darauf hin, dass YouTube wie alle Dienste von Google der einheitlichen Datenschutzerklärung von Google unterfalle.[32] Diese regelt umfassende Datenerhebung und -verwendung für Werbezwecke. Ob die Nutzer hinreichend transparent darüber informiert werden und wirksam einwilligen können sei zweifelhaft. Bezüglich einer älteren Version der Nutzungsbedingungen wurde die Anfang 2019 durch das Kammergericht Berlin verneint.[33]

Besonders hinzuweisen ist auf die bei YouTube ebenfalls zu Facebook vergleichbaren Funktionen des Folgens von bestimmten Profilen, Likens einzelner Beiträge und des Kommentierens, die ebenfalls zu einem erweiterten Aufkommen sensibler Daten führen und die Erstellung von Nutzerprofilen begünstigen.

Bis zum 19. September 2020 muss in den Mitgliedstaaten der EU die neue **Richtlinie für audiovisuelle Mediendienste (AVMD-RL)** umgesetzt werden.[34]

---

31 Ingold, „Polizei 2.0“: Grenzen der behördlichen Öffentlichkeitsarbeit in sozialen Netzwerken, VerwArch 2017, 240, 250 ff.

32 BfDI, Betreiben von Social-Media-Accounts für das Parlament durch die Verwaltung des Deutschen Bundestages, 27.6. 2019, sh. Anlage 3.

33 KG Berlin, Urteil vom 21.3.2019 - 23 U 268/13, juris.

34 Richtlinie (EU) 2018/1808 des Europäischen Parlament und des Rates vom 14. November 2018 zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) im Hinblick auf sich verändernde Marktgegebenheiten.

Des Weiteren ist auf das durch das Bundesverfassungsgericht bestätigte Verbot eines Staatsfernsehens hinzuweisen.[35] Die Problematik ist weitestgehend vergleichbar mit dem Parlamentsfernsehen des Bundestages.[36]

4. Implikation der Grundrechte

Das Datenschutzrecht dient im Wesentlichen dem Schutz des Grundrechts auf **informationelle Selbstbestimmung** (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG).[37] Nach der Rechtsprechung des **Bundesverfassungsgerichts** gibt es **kein belangloses Datum**. Geschützt sind nicht nur sensible Daten, sondern grundsätzlich alle personenbezogenen Daten.

Bei einer elektronischen Datenverarbeitung ergebe sich aus der Speicherung auch großer Mengen von Daten und den vielfältigen Möglichkeiten der Verknüpfung von Daten und Nutzung für Folgeeingriffe sowie des immanenten Missbrauchsrisikos durch Dritte eine besondere Eingriffsqualität.[38] Das Bundesverfassungsgericht betonte im Zusammenhang mit der anlasslosen automatisierten Kennzeichenerfassung, dass es zur Freiheitlichkeit des Gemeinwesens gehöre, dass sich Bürgerinnen und Bürger grundsätzlich fortbewegen können, ohne dabei beliebig staatlich registriert zu werden, hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen zu müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein.[39] **Informationserhebungen** gegenüber Personen, die den Eingriff durch ihr Verhalten nicht veranlasst haben und damit **anlasslos** erfolgen, sind grundsätzlich von höherer Eingriffsintensität als anlassbezogene.[40] Das Bundesverfassungsgericht stellt besondere Anforderungen an die Rechtfertigung solcher Eingriffe. Insbesondere würden polizeiliche Generalklauseln oder die allgemeine Festschreibung des Zweckes der Datenverarbeitung für die gebotene Konkretisierung der Eingriffsschwelle durch den Gesetzgeber nicht genügen.[41]

Im Zusammenhang mit Social-Media-Auftritten von öffentlichen Stellen können sich Grundrechtseingriffe sowohl durch die Verarbeitung sensibler Daten als auch durch die Sammlung und Auswertung von **großen Mengen** von **Daten** einzelner bzw. vieler oder aller Nutzer ergeben. Ferner kann das Risiko unbefugter Zugriffe Dritter bestehen. Zudem kann insbesondere bei Betreibern von Social-Media-Plattformen, die ihren Sitz außerhalb des Anwendungsbereichs der DSGVO haben, oft nur schwer aufgeklärt werden, in welcher Weise diese die Nutzerdaten verarbeiten und ggf.

---

35 BVerfGE 31, 314 (329); 83, 238 (323).

36 Hierzu ausführlich WD 10 - 3000 - 038/11, Gesetzlicher Rahmen für ein Parlamentsfernsehen; zur Frage der Einstufung eines Livestreams der BILD-Zeitung auf YouTube als zulassungspflichtiger Rundfunk vgl. VG Berlin, Beschl. v. 18.10.2018 –VG 27 L 364.18), wonach es vor allem auf das Vorliegen eines Sendeplanes ankommen dürfte.

37 Siehe ausführlich Engeler, Der staatliche Twitter-Auftritt, MMR 2017, 651, 654 ff.

38 BVerfG, NJW 2008, 1505 (1506 Rz. 63 f. und 81) (Hervorhebung nur hier).

39 BVerfG, Beschluss vom 18. Dezember 2018, Az.: 1 BvR 142/15, juris Rz. 51.

40 BVerfG, NJW 2008, 1505 (1507 Rz. 78 m.w.N.).

41 BVerfG, Beschluss vom 18. Dezember 2018, Az.: 1 BvR 142/15, juris Rz. 103, 106.

Dritten zugänglich machen. Es stellt sich ferner die Frage, ob eine anlasslose automatisierte Verarbeitung von Nutzerdaten auf Social-Media-Plattformen etwa zur Erstellung von Nutzerstatistiken ohne weiteres auf die Generalklausel des § 3 BDSG i.V.m. Art. 6 Abs. 1 S. 1 lit. e) DSGVO gestützt werden kann.

Zudem können weitere Grundrechte in bestimmten Konstellationen von besonderer Bedeutung sein. Hingewiesen werden soll hier vor allem auf die Bedeutung der Grundrechte, wenn bestimmte **Beiträge** oder **Nutzer** auf den Social-Media-Accounts der Behörden **gesperrt** werden. Ein Grund dafür kann beispielsweise in der Verbreitung von sog. Hassnachrichten liegen, die über diese Konten für einen großen Personenkreis sichtbar wären. Relevante Grundrechte könnten insofern die **Meinungsfreiheit** (Art. 5 Abs. 1 S. 1 GG) und **Informationsfreiheit** des Nutzers (Art. 5 Abs. 1 S. 1 GG), das Recht auf **gleiche Teilhabe an öffentlichen Leistungen und Einrichtungen** (Art. 5 Abs. 1 S. 1 GG, Art. 3 Abs. 1 GG) und die **Pressefreiheit**, wenn der Nutzer Medienvertreter ist (Art. 5 Abs. 1 S. 2 GG), sein.[42] Eine Rechtfertigung der Eingriffe in diese Grundrechte ist möglich, wenn dem Grundsatz der **Verhältnismäßigkeit** entsprochen wird.

Darüber hinaus können spezielle Situationen auch zu weiteren Eingriffen führen und somit auch eine gesonderte Einschränkung für die Nutzung von Social-Media-Kanälen bedeuten. 2019 hat das OVG NRW entschieden, dass die Polizei keine Fotos von **Versammlungen** auf Twitter und Facebook veröffentlichen darf, auch wenn die Veröffentlichung der Fotos zur Öffentlichkeitsarbeit und der Erfüllung von Informationspflichten erfolgte.[43] Insoweit ist auch die grundrechtlich geschützte Versammlungsfreiheit (Art. 8 Abs. 1 GG) berührt.

Darüber hinaus ist die Staatsgewalt den rechtsstaatlichen Grundsätzen verpflichtet und unterliegt insoweit auch bei der Verbreitung von Informationen den Geboten der **Neutralität**, **Sachlichkeit** und **Richtigkeit**.[44]

5. Weitere Diskussionsansätze

Kritisch gesehen wird darüber hinaus besonders von Wewer[45] der Effekt, dass wenn eine Behörde oder staatliche Einrichtung auf einem bestimmten sozialen Medium vertreten ist, sie dann damit auch für dieses **Werbung** macht bzw. ihm einen gewissen **Anschein der staatlich geprüften unbedenklichen Nutzung** gibt. Zudem weist er darauf hin, dass über die Nutzung von sozialen Medien

42 Wissenschaftliche Dienste des Deutschen Bundestages, Zugang zur Öffentlichkeitsarbeit der Polizei in sozialen Medien („Twitter"), WD 3 - 3000 - 044/18 vom 21.2.2018. Dazu auch: Lüdemann, Grundrechtliche Vorgaben für die Löschung von Beiträgen in sozialen Netzwerken, MMR 2019, 279 ff.; Kalscheuer/Jacobsen, Das digitale Hausrecht von Hoheitsträgern, Unter welchen Voraussetzungen darf der Staat Twitter-Nutzer blockieren?, NJW 2018, 2358 ff.; Milker, Die Polizei auf Twitter – Brauchen wir ein Social-Media-Gesetz für staatliche Stellen?, NVwZ 2018, 1751 ff.; Libertus, Sperren und Löschen von User-Content durch öffentlich-rechtliche Rundfunkanstalten auf deren Social Media-Präsenzen, CR 2019, 262 ff.

43 Dazu OVG NRW, Urteil vom 17.9.2019 – 15 A 4753/18; zur Entscheidung der Vorinstanz: Wendt, Social Media und Polizei, Bildaufnahmen von Versammlungen zur Öffentlichkeitsarbeit, ZD-Aktuell 2019, 06418 (beck-online).

44 Wissenschaftliche Dienste des Deutschen Bundestages, Zugang zur Öffentlichkeitsarbeit der Polizei in sozialen Medien („Twitter"), WD 3 - 3000 - 044/18 vom 21.2.2018. Siehe auch ausführlich: Ingold, „Polizei 2.0": Grenzen der behördlichen Öffentlichkeitsarbeit in sozialen Netzwerken, VerwArch 2017, 240 ff.

45 Wewer, Darf der Staat Facebook und Twitter nutzen?, ZRP 2016, 23 ff.

die Firmen Einblicke in die **behördliche Kommunikation** erhalten könnten, die über die Netzwerke zumeist mit Bürgern erfolge. Die so den Netzwerken zusätzlich ermöglichten Datenerhebungen könnten durch diese auch gezielt kommerziell genutzt werden. Zudem hinterfragt er die Unentgeltlichkeit der Nutzung der sozialen Medien im Rahmen bestehender Regelungen für die öffentliche Hand zur Entgegennahme von Geschenken und der Korruptionsprävention. Insofern empfiehlt er, mit den Anbietern der Netzwerke entgeltliche Verträge zu schließen, bei denen diese sich im Gegenzug verpflichten, auf die Auswertung der Daten zu verzichten.

***