Webcrawling

Praxisrelevante Daten-Analyse im datenschutzrechtlichen Spannungsverhältnis

Alexander Jung

I. Einleitung

98.000 Tweets über den Kurznachrichtendienst Twitter, innerhalb einer Minute.[1] Bereits diese Zahl belegt die immense Datenmenge, welche weltweit über die Echtzeit-Anwendung „gezwitschert" wird. Der Konsument von digitalen Informationen wird zum Prosumenten – dem Produzenten, der gleichzeitig auch konsumiert.

Die darüber entstehende Meinungsvielfalt will unweigerlich aufgenommen und analysiert werden. Ursprünglich wurde die Verfolgung von Stimmungsbildern auf Websites und in Foren als Webmonitoring[2] bezeichnet, woraus sich aufgrund des nicht aufzuhaltenden Siegeszugs von sozialen Medien, besonders in Form von Blogs oder Social Networks, die Begrifflichkeit „Social-Media-Monitoring" festsetzte.

Dabei ist insbesondere beachtlich, dass die Beiträge in den sozialen Netzwerken und Online-Foren die Meinungen, Ansichten und Anschauungen der Nutzer sehr direkt und ungefiltert wiedergeben. Es existiert gerade keine (intendierte) Fragestellung eines Dritten, ein Umstand der etwa in der Markt- und Meinungsforschung regelmäßig von besonderer Relevanz sein kann.

Daneben erweist sich das Internet auch als eine besonders wichtige Informationsquelle für anstehende Kaufentscheidungen. Fast 90% der Internet-Nutzer suchen Informationen für ihre Entscheidungen im Internet.[3] Dabei werden Produktbewertungen, Herstellerwebsites aber auch Kommentare auf Blogs und Foren zu Rate gezogen. In einer Umfrage des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) wurden über 1000 Personen ab 14 Jahren nach ihren Entscheidungshilfsmitteln befragt. Mit 58 Prozent der Befragten rangieren Preisvergleichswebsites noch vor Herstellerwebsites mit 51 Prozent, gefolgt von Blogs und Internetforen mit 35 Prozent.[4]

Alexander Jung, Dipl.-Jurist (Univ.), Managing Consultant der legitimis GmbH für Datenschutz und Compliance im Auftrag namhafter internationaler Konzerne

Obwohl das Bewusstsein geschärft und der Nutzen erkannt ist, fühlen sich Unternehmen bei dem Nachweis ihrer Social-Media-Aktivitäten immer noch überfordert. Dies ergaben die Ergebnisse einer Unternehmensbefragung des Bundesverbands Digitale Wirtschaft (BVDW), wonach eine Mehrzahl der Befragten die Erfolgsmessung als schwierig bis sehr schwierig einstuft.[5] Im Rahmen des Beitrags soll gezeigt werden, welche rechtlichen Leitplanken für das überaus praxisrelevante Spielfeld von Marketing und Marktforschung im Zusammenhang mit Social-Media-Monitoring gesetzt sind und wie ein solches datenschutzrechtlich einwandfrei realisiert werden kann.

1 Abrufbar unter http://www.handelsblatt.com/technik/it-internet/datenflut-was-passiert-in-60-sekunden-im-internet/4274652.html, zuletzt abgerufen am 05.05.2015.

2 *Plieninger/Schapke/Falk*, Webmonitoring und Websitenmonitoring, S. 5.

3 Abrufbar unter http://www.bitkom.org/files/documents/BITKOM_E-Commerce_Studienbericht.pdf, zuletzt abgerufen am 04.05.2015.

4 Abrufbar unter http://www.bitkom.org/files/documents/BITKOM_E-Commerce_Studienbericht.pdf, zuletzt abgerufen am 04.05.2015.

5 Abrufbar unter http://www.bvdw.org/mybvdw/media/download/kompass-social-media-2014-2015.pdf?file=3303, zuletzt abgerufen am 05.05.2015.

II. Problemaufriss & Grundlagen der Technik

Mit dem Social-Media-Monitoring wird das Internet systematisch nach Social-Media-Beiträgen durchsucht. Als rechtliches Risiko stehen hierbei datenschutzrechtliche Gesichtspunkte im Vordergrund. Denn die Erhebung und Nutzung personenbezogener Daten ist nur in engen Grenzen zulässig, etwa wenn Daten allgemein zugänglich sind. So verwundert es nicht, dass der technische Fortschritt rechtliches Sprengpotential liefert. Bei Sozialen Netzwerken, etwa Facebook, ist bereits fraglich, inwieweit die dort veröffentlichten Daten auch im Sinne des Gesetzes öffentlich zugänglich sind. Die Interessen des Einzelnen an einer Nicht-Veröffentlichung von Informationen dürften überwiegen, wenn die Netzwerke privat genutzt werden, wodurch das Erheben personenbezogener Daten in diesem Bereich unzulässig wäre. Beim Social-Media-Monitoring werden zwar keine Primärdaten erhoben, sondern nur aus öffentlichen Daten zusammengeführt. In jedem Fall sind weiterhin die Voraussetzungen des Bundesdatenschutzgesetzes zu beachten.

Obwohl die datenschutzrechtliche Dimension bekannt ist, besteht natürlich ein Bedürfnis zur systematischen Recherche und Auswahl der Informationen, wenn es um die Begeisterung der Community für ein neues Produkt oder die Zielgruppenanalyse bei Einführung einer neuen Marketingkampagne geht.

Die zu diesen Zwecken am Markt verfügbaren Tools ähneln sich in ihrer Funktionsweise stark: Nachdem man Themen und passende Schlagworte (Keywords) festgelegt sowie Ausschlusslisten definiert hat, kann entweder das gesamte Internet nach Suchtreffern durchforstet (Screening) oder nach relevanten Quellen gefiltert (Monitoring) werden. Hierbei wird auf die aus dem Suchmaschinen-Sektor bekannte Crawler-Technologie zurückgegriffen. Diese ist aber insoweit modifiziert, dass anders als bei herkömmlichen Suchmaschinen von der Monitoring-Technologie auch Foren und Micro-Communities vollständig durchforstet werden. Application Programming Interfaces (APIs) bzw. Schnittstellen sorgen dafür, dass die gewünschten Daten aus Social-Media-Portalen den Anbietern bereits entsprechend strukturiert vorliegen. Bei Blogs hingegen wird auf RSS-Feeds zurückgegriffen, welche die Darstellung neuer Bloginhalte ermöglichen. Diese von den Betreibern angebotenen Feeds nutzen die Meta-Suchmaschinen, um die Inhalte zu indexieren.

> „Grundsätzlich gilt deutsches Recht, sobald ein Anbieter von Social-Media-Monitoring-Tools Daten erfasst, die auf in Deutschland gelegenen Servern gespeichert sind."

Zudem unterscheiden sich die Technologien der einzelnen Crawling-Anbieter[6] im Hinblick auf die Suchtiefe des Crawling-Prozesses.

III. Personenbezogene Daten & Anwendbarkeit des BDSG

1. Personenbezogene Daten und Anwendbarkeit

Das Bundesdatenschutzgesetz bezweckt den Schutz des Einzelnen im Umgang mit seinen personenbezogenen Daten und den Schutz vor Beeinträchtigungen seines Persönlichkeitsrechts.[7] Als unproblematisch ist das Social-Media-Monitoring dann anzusehen, wenn die Daten entweder von Beginn an keinen Personenbezug aufweisen, d. h. anonym erhoben werden oder in unmittelbarem Zusammenhang mit der Erhebung anonymisiert werden. In diesen Fällen finden die Bestimmungen des Bundesdatenschutzgesetzes keine Anwendung.[8] Allerdings zeigt der Vorlagebeschluss des Bundesgerichtshof zum Europäischen Gerichtshof zur umstrittenen Frage, ob dynamische IP-Adressen als personenbezogene Daten einzuordnen sind,[9] dass die Linie hier nicht trennscharf gezogen werden kann. Einige Anbieter von Monitoring Tools begeben sich deshalb mit der Aussage, dass personenbezogene Daten trotz Erhebung etwa des Namens nicht im rechtlichen Sinne „erhoben" werden, auf rechtlich unsicheres Terrain. Vielmehr sei der Blick darauf zu wenden, ob etwa aufgrund der Anonymisierung die jeweilige Nutzung zulässig ist. Im Falle der Anonymisierung nach § 3 Abs. 6 BDSG komme es etwa zu einer dauerhaften Löschung der Identifikationsmerkmale, womit eine Anwendung des Bundesdatenschutzgesetzes entfalle. Obwohl viele Nutzer Beiträge und Kommentare unter einem Pseudonym verfassen, werden oftmals private Informationen preisgegeben, vom Wohnort bis zum Geburtstag. Somit werden unter einem Pseudonym erstellte Postings regelmäßig personenbezogene Daten erhalten. Diese Pseudonymität gegenüber dem Plattform-Betreiber stellt sich jedenfalls in Fällen, in denen kein Zusatzwissen hinzugezogen werden kann, als Anonymität gegenüber Dritten dar.

2. Anwendbarkeit des BDSG nach § 1 Abs. 5 BDSG

Neben der technischen Herausforderung, namentlich der Erhebung, Speicherung und Auswertung großer Datenmengen, stellt sich bei der Wahl von Anbietern mit Sitz im Ausland regelmäßig die Frage, welches nationale Recht Geltung entfaltet. Fraglich ist etwa, ob ein Dienstleister aus den USA an deutsches Recht gebunden ist und wenn ja, unter welchen Voraussetzungen. Grundsätzlich gilt deutsches Recht, sobald ein Anbieter von Social-Media-Monitoring-Tools Daten erfasst, die auf in Deutschland gelegenen Servern gespeichert sind. Dabei spielen Foren als Quelle des Monitoring eine bedeutende Rolle.[10] Denn wie gezeigt liefern diese ein äußerst unverfälschtes Bild von Meinungen und Ansichten, nicht verwässert durch die Arten der Fragestellungen von Meinungsforschern.

Insgesamt führt dies aber nicht nur zu Rechtsunsicherheit bei den Verwendern, sondern auch bei den Anbietern aus dem Ausland. Diese sind sich bei der Erhebung der Daten unsicher, in welchen Fällen sie sich bei Zugriff auf Soziale Netzwerke an deutsches Datenschutzrecht zu halten haben.

6 Abrufbar unter http://www.goldbachinteractive.com/aktuell/fachartikel/marktubersicht-plattformen-social-media-monitoring, zuletzt abgerufen am 05.05.2015.

7 *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 1 Rn. 24.

8 *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 3a Rn. 47.

9 BGH, Beschl. v. 24.10.2014 – VI ZR 135/13.

10 Abrufbar unter http://www.tomorrow-focus-media.de/uploads/tx_mjstudien/Social_Media_Effects_2012_neuerMaster.pdf?PHPSESSID=1583a130fcc86866465157cbd42815a5, zuletzt abgerufen am 05.05.2015.

Deutsche Anbieter sind bei datenschutzrechtlichen Problematiken erfahrungsgemäß eher sensibilisiert. So haben viele davon einen Datenschutzbeauftragten bestellt, der eben auch die Problematik der Anwendbarkeit des deutschen Rechts hinterfragen wird.[11]

Näher beleuchtet steht mit § 1 Abs. 5 BDSG auch eine Vorschrift zur Verfügung, welche Vorgaben zur Anwendung von internationalem Datenschutzrecht enthält. Bei Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten in Deutschland durch eine verantwortliche Stelle in einem EU-/EWR-Staat findet das jeweilige nationale Recht Anwendung. Eine Abweichung von diesem Grundsatz gibt es nur, wenn eine Niederlassung in Deutschland die datenschutzrelevanten Aktivitäten betreibt, die verantwortliche Stelle aber in einem anderen EU-EWR-Staat sitzt.

Entscheidend ist nunmehr, ob das Bundesdatenschutzgesetz auch für Anbieter aus Drittstaaten Anwendung findet. Hierzu ist erforderlich, dass entsprechend § 1 Abs. 5 S. 2 BDSG der Anbieter datenschutzrechtlich relevanten Umgang im Inland mit den Daten hat. In Anlehnung an Artikel 4 lit. c RL 95/46/EG bedeutet dies, dass der Verantwortliche aus einem Drittstaat auf Mittel in einem Mitgliedsstaat zurückgreifen muss. Darunter sind etwa körperliche Einrichtungen zu verstehen, die der Verarbeitung personenbezogener Daten dienen,[12] also etwa Server und sonstige EDV-Systeme. Somit kommt es zu einer Anwendung des Bundesdatenschutzgesetzes, wenn Anbieter aus Drittstaaten auf Daten zugreifen, die auf deutschen Servern belegen sind. Umgekehrt kommt es nicht zu einer Anwendung deutschen Datenschutzrechts, wenn der Anbieter in einem Drittstaat ausschließlich Daten erhebt, die dort belegen sind.

IV. Rechtsrahmen

1. Verbotsgesetz mit Einwilligungsvorbehalt

Das Bundesdatenschutzgesetz ist ein Verbotsgesetz mit Einwilligungsvorbehalt.[13] Dies bedeutet, dass entsprechend § 4 Abs. 1 BDSG die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur zulässig ist, wenn eine Einwilligung des Betroffenen vorliegt oder eine Rechtsvorschrift den Datenumgang gestattet.

2. Erlaubnis/Einwilligung

Allerdings wird die Einwilligung in den meisten Fällen als Erlaubnis zur Verarbeitung und Nutzung von Daten ausscheiden, da der Betroffene seine Einwilligung gerade nicht für eine weitere Nutzung durch einen Dritten erteilt, sondern diese an die jeweilige verantwortliche Stelle gebunden hat. Am Beispiel der Allgemeinen Geschäftsbedingungen von Facebook ist etwa festzuhalten, dass das Unternehmen ohne die Erlaubnis keine Informationen an Werbe-, Mess- oder Analysepartner weitergibt, welche die Nutzer persönlich identifizieren.[14] Im Übrigen müsste der Betroffene nicht nur über die Möglichkeit informiert werden, dass seine Daten von Dritten verwendet werden können, sondern es müsste auch ein Hinweis auf die jederzeitige Möglichkeit zum Widerruf erfolgen. Nach § 4a BDSG hat die Einwilligung zudem grundsätzlich schriftlich zu erfolgen. Eine stillschweigende oder mutmaßlich erteilte Einwilligung scheidet aus. Dies ist auch interessengerecht, da dem Betroffenen regelmäßig nicht transparent sein wird, dass seine Daten, Kommentare und veröffentlichten Texte mit Personenbezug auch von Media Monitoring-Anbietern verarbeitet werden (können). Kurzum ist die Einwilligung nicht als praktikable Lösung anzusehen, da sie keine Rechtssicherheit bietet. Von daher muss auf weitere Erlaubnisvorschriften aus dem Bundesdatenschutzgesetz zurückgegriffen werden.

3. Gesetzliche Rechtfertigung

Mangels Praxisrelevanz der Einwilligung bedarf es eines Rückgriffs auf einen gesetzlichen Erlaubnistatbestand im BDSG. In Betracht kommt dabei etwa die Rechtfertigung aus § 28 Abs. 1 S. 1 Nr. 3 BDSG, wonach das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Die Erleichterung für die Verwendung der personenbezogenen Daten in diesem Fall beruht auf der Informationsfreiheit aus Art. 5 Abs. 1 S. 1 GG.[15]

Als allgemein zugänglich sind die Daten dann zu kategorisieren, wenn sie nach ihrer Zielsetzung einem nicht individuell bestimmbaren Personenkreis Informationen vermitteln sollen.[16] Das World Wide Web an sich ist als öffentliche Quelle zu sehen, da der Zugriff für jedermann eröffnet ist.[17] Nach einer Ansicht soll bereits ein Anmeldeerfordernis, etwa ein Log-In bei sozialen Netzwerken dazu führen, dass die Informationen nicht mehr im Rechtssinne öffentlich zugänglich sind.[18] Hiergegen steht aber die Formulierung des § 10 Abs. 5 S. 2 BDSG, woraus abgeleitet werden kann, dass die allgemeine Zugänglichkeit auch dann gegeben ist, wenn die Abrufverfahren *anmeldebedürftig* sind oder wenn der Zugang zu den Daten *kostenpflichtig* ist.[19] Eine Rückausnahme soll jedoch dann gelten, wenn die Daten nicht auf einen bestimmten Nutzerkreis beschränkt wurden.[20] Folglich kann davon gesprochen werden, dass eine Mehrzahl der personenbezogenen Daten in Foren und Blogs öffentlich zugänglich ist. Insbesondere bei Facebook ist eine große Zahl etwa an Pinnwänden-Einträgen frei zugänglich und fällt deswegen unter die Regelung des § 28 Abs. 1 S. 1 Nr. 3 BDSG.

Zu beachten gilt, dass die Erlaubnis insoweit beschränkt ist, als dass ein schutzwürdiges Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle überwiegt. Dabei muss dieses Interesse offensichtlich überwiegen, wobei eine intensive Einzelfallprüfung entbehrlich ist.[21] Abweichend von der Prüfung in § 28 Abs. 1 S. 1 Nr. 2 BDSG sind die Voraussetzungen auch höher, weil durch die Zugänglichkeit der Daten der Betroffene weniger schutzbedürftig ist.[22] Deswegen muss das Betroffeneninteresse deutlich höher als jenes der verarbeitenden Stelle und ohne nennenswerte Einzelfallprüfung leicht erkennbar sein.[23]

> „Es bestehen Gestaltungsspielräume, um Webcrawling auf ein sicheres datenschutzrechtliches Fundament zu stellen."

Insgesamt ist die Intention der Regelung, dass allgemein zugängliche Informationen weitgehend verwendet werden dürfen.

In Abgrenzung zu § 28 BDSG ist § 30a BDSG anzuwenden, sobald Datenmaterial verwendet wird, welches bei der verantwortlichen Stelle nicht ursprünglich für einen anderen Zweck, sondern erstmalig erhoben wurde.[24] Damit wird diese Regelung relevant, sobald das Monitoring von Anbietern zum Zweck der Meinungsforschung eingesetzt wird. Insbesondere das Wettbewerbs- und Kampagnenmarketing tritt dabei für das eigene Marketing in den Vordergrund. Denn die Strategie der Wettbewerber eröffnet die Möglichkeit, rasch auf die Reaktionen des Marktes zu reagieren. Zudem werden Unternehmen dadurch in die Lage versetzt, die Aufstellung des eigenen Unternehmens im Bereich Werbung prüfend zu hinterfragen und gemäß den Reaktionen der Nutzer anzupassen. Die Markenkommunikation wird darauf ausgerichtet, wie die Marke bei den Nutzern ankommt, insbesondere wie Meinungsführer sich dazu positionieren. Neben klassischem Marketing nutzen Unternehmen die Analyse der Sozialen Medien auch, um den Erfolg von Nachhaltigkeitskampagnen oder sozialem Engagement sichtbar zu machen.

Auf Tatbestandsebene ist zusätzlich der in § 30a Abs. 2 S. 1 BDSG niedergelegte Grundsatz der Zweckbindung zu beachten, wonach für die Markt- oder Meinungsforschung erhobene oder gespeicherte personenbezogene Daten nur für diese Zwecke verarbeitet oder genutzt werden dürfen. Dieser Zweckbindungsgrundsatz wird nur dann durchbrochen, wenn Daten aus allgemein zugänglichen Quellen erhoben wurden.

Nach § 30a Abs. 1 S. 1 Nr. 2 BDSG ist das geschäftsmäßige Erheben, Verarbeiten oder Nutzen personenbezogener Daten für Zwecke der Markt- oder Meinungsforschung zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen durfte und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung gegenüber dem Interesse der verantwortlichen Stelle nicht offensichtlich überwiegt. Wie bereits ausgeführt, wird in einer Vielzahl der Fälle die öffentliche Zugänglichmachung im Rahmen von Blog- und Forenbeiträgen bejaht werden können. Unterscheiden kann man also auf der Basis der geschlossenen Foren, die nur durch ein entsprechendes Passwort für den Monitoring-Anbieter sichtbar gemacht werden können. Hier fehlt es an der allgemeinen Zugänglichkeit. Überdies ist aber zu beachten, dass das Interesse der verantwortlichen Stelle mit dem Betroffeneninteresse abgewogen werden muss. Dabei wird das schutzwürdige Interesse des Betroffenen beispielhaft dann offensichtlich überwiegen, wenn er bereits bei einer Vorerhebung die Mitwirkung an der Markt- und Meinungsforschung verweigert hat.[25] Insofern ist sicher zu stellen, dass die vorherige Verweigerung berücksichtigt und technisch sichergestellt wird, dass die Daten nicht für die Markt- und Meinungsforschung genutzt werden.

Unter Zuhilfenahme von § 30a Abs. 3 BDSG sollen die in zulässiger Weise erhobenen Daten frühestmöglich anonymisiert werden. Dabei wird die Anonymisierung dadurch sichergestellt, dass aus den einzelnen Angaben der Betroffenen keine Rückschlüsse mehr auf deren konkrete Identität möglich sind.[26] Die dadurch gewonnen Datensätze unterliegen dann nicht (mehr) dem Bundesdatenschutzgesetz.

V. Datenschutzrechtliche Grundsätze

1. Zweckbindungsgrundsatz

Nach dem Zweckbindungsgrundsatz sind personenbezogene Daten nur für den Zweck zu verwenden, für welchen sie ursprünglich erhoben wurden.[27] Allerdings sind Zweckentfremdungen bei Vorliegen einer gesetzlichen Erlaubnis gestattet. Der Zweckbindungsgrundsatz wird in § 28 Abs. 1 S. 2 BDSG deklaratorisch benannt. Der Zweck ist dabei umso mehr zu konkretisieren, je stärker die Belastung für den Betroffenen ist.[28] Mit Blick auf die Möglichkeiten des Social-Media-Monitoring hat sich auch hier die Zweckdefinition daran zu orientieren, welche Arten von Daten erhoben werden.

2. Direkterhebungsgrundsatz

Im Bundesdatenschutzgesetz gilt der Grundsatz der Direkterhebung – in § 4 Abs. 2 BDSG verankert –, also die Vorgabe, die Daten des Betroffenen direkt bei diesem zu erheben und nicht über den Umweg der Einschaltung eines Dritten zu sammeln, zu speichern oder zu verarbeiten.[29] Grundsätzlich sind die Daten also mit seiner Mitwirkung in Form der Einwilligung oder auf Grundlage einer gesetzlichen Erlaubnis, regelmäßig mit seiner Kenntnis zu erheben.[30]

3. Zusammenführungsverbot

Überdies besteht noch das Zusammenführungsverbot im Bereich der Werbung und Marktforschung, wonach einmal pseudonymisierte Daten gemäß § 15 Abs. 3 S. 3 Telemediengesetz (TMG) nicht mit anderweitigen Daten über die unter einem Pseudonym geführte Person zusammengeführt werden dürfen. Hiermit könnten die so erfassten Daten einer bestimmbaren Person zugeordnet werden. Ein Umstand, der gerade verhindert werden bzw. nur mit der Einwilligung des Betroffenen ermöglicht werden soll.

11 Vergleich verschiedener Anbieter und deren Angaben auf der jeweiligen Anbieter-Website.
12 *Gabel*, in: Taeger/Gabel, BDSG § 1 Rn. 58; *Dammann*, in: Simitis, BDSG, 8. Aufl. 2014, § 1 Rn. 220.
13 *Gola/Schomerus*, Bundesdatenschutzgesetz, 12. Aufl. 2015, § 4 Rn. 3.
14 Abrufbar unter https://www.facebook.com/about/privacy/, zuletzt abgerufen am 20.05.2015.
15 *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 28 Rn. 150.
16 BVerfG, Urt. v. 03.10.1969 – 1 BvR 46/65 = BVerfGE 27, 71, 83; *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 28 Rn. 151.
17 OLG Hamburg, Urt. v. 13.11.2009 – 7 W 125/09 = MMR 2010, 63.
18 *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 4. Auflage 2014, § 28 Rn. 58.
19 *Von Lewinski*, in: Beck'scher Online-Kommentar Datenschutzrecht, 11. Edition Stand: 01.02.2015, § 10 Rn. 46.
20 *Ernst*, NJOZ 2011, 953, 955; *Bissels/Lützeler/Wisskirchen*, BB 2010, 2433, 2437.
21 *Wolff*, in: Beck'scher Online-Kommentar Datenschutzrecht, 11. Edition Stand: 01.05.2013, § 28 Rn. 89.
22 *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 28 Rn. 162.
23 *Wolff*, in: Beck'scher Online-Kommentar Datenschutzrecht, 11. Edition Stand: 01.05.2013, § 28 Rn. 89.
24 *Ehmann*, in: Simitis, BDSG, 8. Aufl. 2014, § 30a Rn. 33.
25 *Forgó*, in: Beck'scher Online-Kommentar Datenschutzrecht, 11. Edition Stand: 01.02.2015, § 30a Rn. 37.
26 *Forgó*, in: Beck'scher Online-Kommentar Datenschutzrecht, 11. Edition Stand: 01.02.2015, § 30a Rn. 47.
27 *Wolff*, in: Beck'scher Online-Kommentar Datenschutzrecht, 9. Edition Stand: 01.05.2013, Syst A. Rn. 11.
28 *Wolff*, in: Beck'scher Online-Kommentar Datenschutzrecht, 9. Edition Stand: 01.05.2013, Syst A. Rn. 19.
29 *Scholz/Sokol*, in: Simitis, BDSG, 8. Aufl. 2014, § 4 Rn. 19 ff.
30 *Gola/Schomerus*, Bundesdatenschutzgesetz, 12. Aufl. 2015, § 4 Rn. 19.

VI. Auftragsdatenverarbeitung

Zu beachten ist aber, dass es sich um eine Auftragsdatenverarbeitung handeln könnte. Danach wären die beauftragenden Unternehmen auch bei Einschaltung von Monitoring-Anbietern weiterhin zur Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Eine Auftragsdatenverarbeitung im Sinne von § 11 BDSG ist in Abgrenzung zur Funktionsübertragung anzunehmen, wenn der Auftraggeber bestimmte Datenverarbeitungsvorgänge nach vordefinierter Entscheidungs- und Weisungsbefugnis in Auftrag gibt, die ansonsten durch ihn selbst durchgeführt würden.[31] Damit kommt es auf den Einzelfall an, ob also der Auftraggeber die einzelnen Arbeitsschritte vorschreibt, etwa aus welchen Quellen die Erhebung stattfinden soll oder ob er im Zuge eines detaillierten Weisungskonzepts Einfluss auf die Erhebung, Verarbeitung und Speicherung der Daten hat.

VII. Hindernisse & Grenzlinien im Marketing

Mit Blick auf den Grundsatz der Zweckbindung muss natürlich im Kontext zu Big Data besonders sensibel darauf geachtet werden, wie die gefilterten Daten weiterverwendet werden. Der Verführung, auf Grundlage detaillierter Auswertungen individualisiertes E-Mail-Marketing zu betreiben, darf nicht nachgegeben werden. Es gelten insoweit dieselben Grundsätze wie auch bei der „klassischen" Erhebung von Daten und deren späterer Verwendung, insbesondere § 7 UWG. Eine hiernach erforderliche Einwilligung dürfte in den seltensten Fällen vorliegen, ein Nachweis im Wege des „Double-Opt-In" scheidet aus. Mit Blick auf § 15 Abs. 3 TMG eröffnet die Möglichkeit der pseudonymen Erstellung von Interessenprofilen keine rechtssichere Grundlage für das E-Mail-Marketing, da wie eben dargestellt, die gesammelten Daten nach § 15 Abs. 3 S. 3 TMG gerade nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden dürfen und der Nutzer über sein Widerspruchsrecht nicht aufgeklärt wurde.

VIII. Fazit und Handlungsempfehlung

Wie gezeigt, bestehen Gestaltungsspielräume, um das Webcrawling auf ein sicheres datenschutzrechtliches Fundament zu stellen und die Vorgaben zu erfüllen. Es kann bereits in den Voreinstellungen vermieden werden, dass es überhaupt zur Erhebung von personenbezogenen Daten kommt oder eben durch den Einsatz von Anonymisierungsmechanismen die Anwendbarkeit des Bundesdatenschutzgesetzes ausgeschlossen werden. Insgesamt kann bereits bei der Auswahl der Monitoring-Anbieter ein erster Schritt für eine rechtlich einwandfreie Datenverwendung im Unternehmen gelegt werden. Daraus ergibt sich ein starker vertrauensbildender Aspekt mit Werbewirkung gegenüber den Kunden. Mit der steigenden Wahrnehmung des Themas Datenschutz in der Öffentlichkeit geht auch die weitsichtige Planung einher, datenschutzrechtliche Vorgaben im gesamten Unternehmen – und nicht nur sektoral – umzusetzen. Das beginnt bei der aufgezeigten Auswahl des Anbieters und führt bis zum Abschluss einer Vereinbarung zur Auftragsdatenverarbeitung, soweit diese erforderlich wird.

Obwohl das Social-Media-Monitoring keinen Eingang ins Gesetz gefunden hat, kann man dies mit dem vorhandenen rechtlichen Instrumentarium gut in den Griff bekommen. Wie aufgezeigt sind deutsche Anbieter bei datenschutzrechtlichen Problematiken eher sensibilisiert, da viele erstens einen Datenschutzbeauftragten bestellt haben und sich zweitens ihre Server in Deutschland befinden. Deswegen sollte man bei der Auswahl des Anbieters entsprechend hinterfragen, inwieweit er sich an das deutsche Datenschutzrecht gebunden fühlt und Entsprechendes auf seiner Website nach außen kommuniziert.

31 *Gola/Schomerus*, Bundesdatenschutzgesetz, 12. Aufl. 2015, § 11 Rn. 3.

PRIVACY COMPLIANCE

Personenbezogene Daten für Marketingzwecke erwerben und einsetzen: die datenschutzrechtlichen Grenzen

Simone Rosenthal und *Raphael Hoffmann*, Berlin

Wie können personenbezogene Daten rechtskonform für Marketingzwecke erworben und eingesetzt werden? Der Beitrag zeigt auf, was Werbende beim Erwerb und beim Einsatz personenbezogener Daten beachten müssen – von der Erhebung der Daten bis zur Vorbereitung der Werbemaßnahme.

Simone Rosenthal ist Rechtsanwältin und Partnerin bei Schürmann Wolschendorf Dreyer RAe sowie Geschäftsführerin der ISiCO Datenschutz GmbH.

Raphael Hoffmann, M.B.L., ist Datenschutzberater bei der ISiCO Datenschutz GmbH.

I. Einleitung

In einer Zeit, in der auf der einen Seite die Bereitschaft des Einzelnen wächst, persönliche Daten über vermeintlich kostenfreie soziale Netzwerke und/oder vermeintlich kostenfreie Apps preiszugeben[1] und auf der anderen Seite Big-Data- und Data-Mining-Technologien detaillierte Profilbildungen ermöglichen,[2] steigt der Wunsch vieler Unternehmen, die gewonnenen Informationen gewinnbringend für Marketingzwecke zu nutzen. Die *bedarfsspezifische Kundenansprache* minimiert Streuverluste und reduziert Kosten.[3] Je detaillierter die Daten über eine Person sind, desto „persönlicher" lässt sich die Kommunikation zwischen Betroffenem und Unternehmen gestalten. So werden Apps, die den Betroffenen räumlich verorten können, für diesen zum „ständigen Wegbegleiter", über den der App-Betreiber ortsabhängige Angebote schalten kann („Location Based Marketing"). Der *kommunikative Graben* zwischen Unternehmen und betroffener Person schwindet dank neuer Technologien kontinuierlich. Unternehmen und Betroffener werden zu Vertrauten.

Der Aufbau persönlicher Kundenbeziehungen setzt freilich voraus, dass ausreichend personenbezogene Daten verfügbar sind. Hier stellt sich die Frage nach der *Datenquelle*. Nicht jede mögliche Quelle liefert solche Daten, die für das Unternehmen wertvoll sind. Längst geht es im professionellen Marketing nicht mehr nur darum, einen Haufen unstrukturierter Emailadressen zu erwerben. Zunehmend gefragt sind vielmehr Daten, aus denen sich bereits schließen lässt, ob eine Kundenansprache kommerzielles Potential birgt oder nicht.[4]

Das Anreichern des Werbedatenbestands unterliegt dabei strengen datenschutzrechtlichen Erhebungs- und Verarbeitungsregeln. Dies betrifft nicht nur den Datenerwerb von Datenhändlern oder vom Be-

1 Zum Konzept von „Privacy by Contract" siehe neuerdings *Reiners*, Datenschutz in der Personal Data Economy. Eine Chance für Europa, ZD 2015, 51.

2 Zu den gesellschaftlichen Auswirkungen siehe *Geis*, Unternehmen in der Flut elektronischer Kommunikation. Aktuelle Aspekte des Datenschutzes, ZD 2013, 593 ff.

3 „Entscheidend ist [...], dass die Werbebotschaft das wirkliche Interesse des Konsumenten trifft. Nur so kann er positiv überrascht und aufmerksam gemacht werden." *Grages*, Marketing per Datenanalyse und Zielgruppenbildung, DSRITB 2013, 815.

4 Vgl. das „Tippgeber"-System der Debeka, das im letzten Jahr Gegenstand einer Datenschutzprüfung durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz war und mit einer einvernehmlichen Absprache beendet wurde: https://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2014122901 (Abruf: 18.05.2015).