23850

ZD
ZEITSCHRIFT FÜR DATENSCHUTZ

AUS DEM INHALT

www.zd-beck.de

Seiten 541–588
2. Jahrgang 3. Dezember 2012
Verlag C.H.Beck München

12/2012

O850201212

CHRISTIAN SOLMECKE / JAKOB WAHLERS

Rechtliche Situation von Social Media Monitoring-Diensten

Rechtskonforme Lösungen nach dem Datenschutz- und dem Urheberrecht

Marktforschungsinstrument
Social Web
Einwilligung
Direkterhebung
Originalquellen

■ Social Media Monitoring ist längst ein gängiges Marktforschungsinstrument für viele Unternehmen. Dabei werden systematisch Beiträge in sozialen Netzwerken, Blogs, Foren und Micro-Blogging-Diensten (z.B. Twitter) beobachtet und analysiert, um ein Bild über den Meinungsstand im Social Web zu erlangen. Viele Unternehmen greifen für das Social Media Monitoring auf externe Dienstleister zurück, die sich auf diesem Gebiet spezialisiert haben. Dieser Beitrag möchte zunächst die Grundlagen des Monitoring verdeutlichen (unter I.) und die mit dieser Dienstleistung verbundenen datenschutzrechtlichen (unter II.) und urheberrechtlichen (unter III.) Probleme beleuchten. Zudem sollen Praxishinweise zum rechtskonformen Monitoring gegeben werden (unter IV). Um die Darstellung nicht ausufern zu lassen, beschränkt sich dieser Beitrag auf die Hauptfelder der Anbieter, nämlich das Monitoring von Foren, Blogs, Facebook und Twitter.

■ Social media monitoring has long been a usual instrument for market research for many companies. In this, comments on social networks, blogs, forums and micro blogging services (e.g. Twitter) are systematically observed and analyzed in order to obtain a picture of the opinion status on the social web. Many companies use external service providers for social media monitoring which have specialized in this area. This article will first illustrate the basis of monitoring (I.), and then illuminate the data protection law problems connected to these services (II.), as well as the copyright problems (III.). Additionally, practical tips for legally conform monitoring will be presented (IV.). In order for this illustration to not get out of hand, this article will focus on the main areas of the providers, namely monitoring forums, blogs, Facebook and Twitter.

I. Grundlagen des Social Media Monitoring

Social Media ist aus dem Alltag vieler Deutschen nicht mehr wegzudenken. Sie nutzen soziale Netzwerke, Blogs und Foren dabei nicht zur Kommunikation, sondern immer mehr auch zur Information über Produkte und Dienstleistungen. In der repräsentativen Studie „Social Media Atlas 2011"[1] gaben 76% der Befragten an, eine Kaufentscheidung auf Grund einer Empfehlung von privaten Kontakten auf einer Social Media-Plattform getroffen zu haben, während lediglich 21% auf Grund einer dort geschalteten Werbeanzeige zu einem Kauf animiert wurden. Die Zahlen verdeutlichen, dass es für Unternehmen immer wichtiger wird, Beiträge im Social Web systematisch zu beobachten und zu analysieren. So kann ohne aufwändige Konsumentenbefragung herausgefunden werden, wie die Kunden auf ein Angebot reagieren. Diese systematische Beobachtung des Social Web wird Social Media Monitoring genannt.

Mittlerweile befinden sich zahlreiche Anbieter am Markt, die professionelles Monitoring anbieten.[2] Diese indexieren eine große Anzahl verschiedener Quellen. Neben Blogs und Foren werden insbesondere auch *Facebook*-Seiten von Unternehmen und *Twitter*-Nachrichten durchsucht. Die Anbieter speichern die darin befindlichen Inhalte und bewerten sie automatisiert oder manuell. So steht dem Kunden am Ende eine nach Schlüsselwörtern (Keywords) durchsuchbare Datenbank zur Verfügung, mit welcher er sich ein Bild über den Meinungsstand im Social Web machen kann.

Zur Erfassung der Daten bedienen sich die Monitoring-Anbieter verschiedener Technologien. Blogs bieten häufig einen standardisierten Zugriffskanal, den sog. RSS-Feed an, um Inhalte ohne Designelemente einer Website bereitzustellen. Foren hingegen werden mittels einer speziellen Spider-Technologie durchsucht, welche – anders als gewöhnliche Suchmaschinen – die Struktur eines Forums erkennt und entsprechend auswertet. Auf *Facebook*-Seiten und *Twitter* greifen die Monitoring-Anbieter wiederum über eine Schnittstelle (API) zu, um an die Inhalte zu gelangen. Erfasst werden neben den Beiträgen auch das Erstellungsdatum, der Klarname (insbesondere bei Blogs und *Facebook*-Seiten) bzw. das Pseudonym (inbesondere bei Foren und bei *Twitter*) des Autors und die Anzahl der Kommentare.

---

1 Abrufbar unter: http://de.slideshare.net/faktenkontor/social-media-atlas-2011-10599176.

2 Marktübersicht abrufbar unter: http://www.social-media-magazin.de/index.php/inhalt/social-media-monitoring-anbieter.html.

Bei manchen Quellen existieren technische Hürden, mit welchen die Indexierung durch Suchmaschinen verhindert werden soll. So kann z.B. ein Blogbetreiber in einer Datei auf seinem Server, der robots.txt, durch entsprechende Eintragungen festlegen, ob und welche Suchmaschinen Zugriff auf die Inhalte haben sollen. Auch einige – aber längst nicht alle – Monitoring-Anbieter beachten diese Zugriffsschranken bei ihrem Indexierungsprozess.

Die erfassten Daten werden in Datenbanken auf den Servern der Anbieter gespeichert und weiterverarbeitet. Dabei werden die erfassten Beiträge automatisiert oder manuell auf ihre Tonalität (positiv/negativ/neutral) hin untersucht und entsprechend aufbereitet. Die Kunden können dann über eine spezielle Web-Oberfläche Zugriff auf die aufbereiteten Daten nehmen und die Ergebnisse des Monitoring betrachten.

Diese kurze Einführung zeigt bereits, dass Monitoring-Anbieter bei der Erfassung von Social Media-Beiträgen unweigerlich auch personenbezogene Daten bzw. urheberrechtlich geschütztes Material in ihre Datenbanken aufnehmen. Daher soll im Folgenden untersucht werden, auf Grund welcher Rechtsgrundlage dies erfolgen kann.

II. Datenschutzrecht

1. Anwendbarkeit des BDSG

Da die Monitoring-Anbieter vielfach aus dem Ausland operieren, stellt sich zunächst die Frage nach der Anwendbarkeit des deutschen Datenschutzrechts auf die Tätigkeit der Monitoring-Anbieter. Ausgangspunkt der Beantwortung dieser Frage ist § 1 Abs. 5 BDSG. Dieser regelt in Umsetzung der EG-Datenschutzrichtlinie[3] (DS-RL) als Kollisionsvermeidungsnorm, welches Recht bei grenzüberschreitenden Sachverhalten anzuwenden ist. Dabei geht das BDSG grundsätzlich vom Territorialprinzip aus, welches aber für den grenzüberschreitenden Datenverkehr im Bereich der Europäischen Union (EU) bzw. im Europäischen Wirtschaftsraum (EWR) durch das Niederlassungsprinzip durchbrochen wird.[4]

Damit unterliegt jede verantwortliche Stelle, welche mit personenbezogenen Daten in Deutschland umgeht, den Regelungen des BDSG. Anderes gilt nur, wenn die verantwortliche Stelle ihren Sitz innerhalb des EU-/EWR-Raums hat. In diesem Fall gilt in Übereinstimmung mit der DS-RL das jeweilige nationale Recht.[5] Eine Rückausnahme besteht wiederum dann, wenn die verantwortliche Stelle zwar ihren Sitz im EU-Ausland hat, aber die datenschutzrelevante Aktivität durch eine Niederlassung in Deutschland ausgeübt wird. Hier gilt gem. § 1 Abs. 5 Satz 1 BDSG wiederum das deutsche Datenschutzrecht.[6]

Fraglich ist, ob das BDSG auch auf Anbieter Anwendung findet, welche außerhalb der EU bzw. des EWR ihren Sitz haben. Gem. § 1 Abs. 5 Satz 2 BDSG ist dies der Fall, wenn Anbieter „im Inland" mit personenbezogenen Daten umgehen. Wann eine solche datenschutzrelevante Aktivität „im Inland" vorliegt, ist im BDSG nicht geregelt, sondern durch eine richtlinienkonforme Auslegung zu ermitteln.[7] Nach Art. 4 Abs. 1 lit. c der DS-RL ist das jeweilige Datenschutzrecht des Mitgliedstaats anzuwenden, wenn Anbieter aus Drittstaaten auf Mittel zurückgreifen, die sich im Hoheitsgebiet des jeweiligen Mitgliedstaats befinden. „Mittel" im Sinne dieser Vorschrift sind Computer, Server und sonstige Datenverarbeitungsgeräte, die sich der Anbieter nutzbar macht.[8] Nach diesen Grundsätzen lässt sich für Monitoring-Anbieter festhalten: Das BDSG findet auf Monitoring-Anbieter mit Sitz oder datenverarbeitender Niederlassung in Deutschland Anwendung. Ebenso müssen Monitoring-Anbieter aus Drittstaaten, welche ihre Daten von Servern aus Deutschland beziehen bzw. Daten auf deutschen Servern verarbeiten, die Regeln des BDSG einhalten. Außerhalb des Anwendungsbereichs bewegen sich hingegen Monitoring-Anbieter aus Drittstaaten, welche lediglich Daten in Drittstaaten erheben. Erhebt z.B. ein US-Monitoring-Anbieter Daten bei *Facebook* (Serverstandort: USA), so findet das BDSG selbst dann keine Anwendung, wenn es sich um Daten deutscher Staatsangehöriger handelt.

Außerhalb des Anwendungsbereichs des BDSG, insbesondere bei der zivilrechtlichen Verfolgung der durch den unerlaubten Datenumgang begangenen Persönlichkeitsrechtsverletzung, ist die allgemeine Kollisionsnorm des Art. 40 EGBGB anzuwenden. Danach richtet sich das anwendbare Recht nach dem Ort der Verletzungshandlung.[9] Dies ist regelmäßig der Geschäftssitz des Anbieters als Handlungsort. Darüber hinaus kommt auch der Aufenthaltsort des Verletzten als Erfolgsort in Betracht. Dies gilt jedenfalls dann, wenn der Anbieter an diesem Ort seine Dienste planmäßig anbietet.[10]

Für Unternehmen, welche die Leistungen von Monitoring-Anbietern in Anspruch nehmen, gelten die vorstehenden Ausführungen entsprechend. Haben sie ihren Sitz bzw. ihre Niederlassung in Deutschland, so müssen sie die Regeln des BDSG beachten. Allerdings wird dies im Regelfall kein Problem darstellen, da wegen des Grundsatzes der frühestmöglichen Anonymisierung (s. unten II. 2. c)) im Stadium der Datenübermittlung an die Unternehmen keine personenbezogenen Daten mehr vorliegen dürfen und deshalb ein Datenumgang uneingeschränkt möglich ist.

2. Verbot mit Erlaubnisvorbehalt

Nach § 4 BDSG dürfen personenbezogene Daten nur dann erhoben, verarbeitet oder genutzt werden, wenn der Betroffene eingewilligt hat oder eine Rechtsvorschrift dies erlaubt. Als Ausfluss des Grundrechts auf informationelle Selbstbestimmung ist damit der Umgang mit personenbezogenen Daten unter ein generelles Verbot mit Erlaubnisvorbehalt gestellt. Dieses gilt auf jeder Stufe der Datenverwendung, sodass jeder Schritt des Monitoring (Datenerhebung, Datenspeicherung, Datenverarbeitung, Datenauswertung, Datenweitergabe) gesondert zu prüfen ist.

a) Personenbezogene Daten

Das BDSG reglementiert nur die Verwendung personenbezogener Daten. Nach § 3 Abs. 1 BDSG sind dies „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person".

Personenbezogen sind damit nur die Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Das ist einerseits der Fall, wenn Daten mit dem Namen des Betroffenen versehen sind oder sich dieser Zusammenhang aus den Daten unmittelbar ableiten lässt. Andererseits sind auch solche Daten personenbezogen, aus denen der Betroffene bestimmbar ist. Die Bestimmbarkeit entfällt dabei nicht erst, wenn sie absolut unmöglich ist, sondern bereits dann, wenn das Risiko der Bestimmbarkeit verschwindend gering ist.[11] Es kommt demnach auf die Möglichkeiten und das Wissen der verantwortlichen

3 RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
4 *Jotzo*, MMR 2010, 232, 234.
5 BT-Drs. 14/4329, S. 31; *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 1 Rdnr. 198.
6 BT-Drs. 14/4329, S. 31.
7 *Jotzo*, MMR 2010, 232, 236.
8 *Jotzo*, MMR 2010, 232, 236; Ott, MMR 2009, 158, 160.
9 *Hoeren*, Skript Internetrecht, Stand: Oktober 2011, S. 398, abrufbar unter: http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Internetrecht_Oktober_2011.pdf.
10 *Jotzo*, MMR 2010, 232, 233.
11 *Dammann* (o. Fußn. 5), § 3 Rdnr. 23.

Stelle an, sodass dieselben Daten für eine Stelle personenbezogen, für die andere Stelle nicht personenbezogen sein können.

Nach diesen Grundsätzen muss in der Praxis des Monitoring zwischen den verschiedenen Quellen unterschieden werden. Werden Beiträge von *Facebook*-Pages erfasst, so sind die gewonnenen Daten nahezu zu 100% personenbezogen, da auf *Facebook* der Großteil der Nutzer unter ihrem Klarnamen auftritt. Auch beim Monitoring von Blogs können personenbezogene Daten anfallen, wenn die Autoren die Artikel unter ihrem Klarnamen veröffentlichen oder eine Identifikation der Autoren über das Impressum möglich ist. Gleiches gilt für die Erfassung von *Twitter*-Nachrichten, wenn ein Personenbezug z.B. über die angegebene Homepage möglich ist. Werden Foren vom Monitoring erfasst, dürften dagegen kaum personenbezogene Daten anfallen, da die Mitglieder hier traditionell unter einem Pseudonym auftreten.

b) Einwilligung des Betroffenen

Liegen personenbezogene Daten vor, so dürfen diese grundsätzlich nur mit einer schriftlichen Einwilligung des Betroffenen gem. § 4a BDSG verwendet werden. Eine ausdrückliche schriftliche Einwilligung in die Verwendung der Daten durch Monitoring-Anbieter wird dabei in aller Regel nicht vorliegen und wäre auch unpraktikabel. Bei Vorliegen von besonderen Umständen kann gem. § 4a Abs. 1 Satz 2 BDSG auch von der Schriftform abgewichen werden. An deren Stelle kann allerdings nach einhelliger Ansicht nur eine ebenso klare ausdrückliche Erklärung treten. Eine konkludente, stillschweigende oder mutmaßliche Einwilligung kann dagegen hierfür nicht ausreichen.[12] Dieser Ansicht ist auch im Bereich des Monitoring zu folgen, denn ein User, der einen Text ins Social Web stellt, hat in der Regel keine Vorstellung davon, dass Monitoring-Anbieter diesen Text herunterladen, speichern und weiterverarbeiten. Ein mutmaßlicher Wille des Users hinsichtlich der Verwendung seiner Daten durch Monitoring-Anbieter dürfte dementsprechend nicht konstruierbar sein.

c) Gesetzliche Befugnis

Da es nach dem oben Gesagten regelmäßig an einer Einwilligung des Betroffenen nach §§ 4 Abs. 1, 4a BDSG fehlt, kommt nur eine gesetzliche Befugnis zur Verwendung personenbezogener Daten in Betracht. Im Bereich der Datenverarbeitung durch private Stellen enthalten die §§ 28 ff. BDSG Erlaubnisnormen. Welche Erlaubnisnorm letztlich Anwendung findet, richtet sich maßgeblich nach dem Zweck, der mit der Datenverwendung erreicht werden soll. Da das Monitoring hauptsächlich zum Zweck der Markt- und Meinungsforschung betrieben wird, geht diese Darstellung nur auf die speziell hierfür geschaffene Erlaubnisnorm des § 30a BDSG ein.

§ 30a BDSG enthält eine vorrangige Spezialregelung zu § 29 BDSG, wenn die Daten für Zwecke der Markt- und Meinungsforschung verwendet werden sollen. Zu beachten ist für die Monitoring-Anbieter zunächst die Zweckbindungsvorschrift des § 30a Abs. 2 Satz 1 BDSG. Danach dürfen Daten, welche für die Markt- und Meinungsforschung erhoben oder gespeichert wurden, lediglich für diese Zwecke weiterverarbeitet oder genutzt werden. Nicht zulässig ist es daher, die für Markt- und Meinungsforschung erhobenen Daten (auch) für Werbezwecke zu nutzen.[13] Soll eine werbliche Nutzung der Daten erfolgen, so müssen vielmehr bereits bei der Erhebung die strengeren Regelungen des § 29 BDSG beachtet werden.

§ 30a BDSG nennt zwei Fälle des zulässigen Datenumgangs ohne Einwilligung des Betroffenen. Im ersten Fall (§ 30a Abs. 1 Satz 1 Nr. 1 BDSG) ist die Datennutzung erlaubt, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung der Daten hat. Die beiderseitigen Interessen sind hier in Anwendung des Verhältnismäßigkeitsgrundsatzes gegeneinander abzuwägen, wobei das Interesse des Betroffenen schon dann schutzwürdig ist, wenn die Interessen gleichrangig sind.[14] Auf Seiten des Betroffenen ist dabei vor allem die Grundannahme des § 1 Abs. 1 BDSG zu berücksichtigen, dass jeder Umgang mit personenbezogenen Daten ein Eingriff in das Persönlichkeitsrecht (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG) darstellt. Ausfluss dieses Persönlichkeitsrechts ist u.a., dass der Einzelne Herr über seine persönlichen Daten ist und ihm die Rechte über die Verbreitung dieser Daten zustehen.[15]

Unter Berücksichtigung dieser Grundsätze ist eine Datenverwendung durch Monitoring-Anbieter nicht nach § 30a Abs. 1 Nr. 1 BDSG zu rechtfertigen. Mitglieder von sozialen Netzwerken oder anderen Social Media-Plattformen haben in der Regel kein Interesse daran, dass ihre Daten ohne ihr Zutun von Drittunternehmen gespeichert und verarbeitet werden, welche sie überhaupt nicht kennen und deren Leistungen sie nie unmittelbar in Anspruch nehmen. Seitens der Monitoring-Anbieter lässt sich dagegen kaum ein schutzwürdiges Interesse konstruieren. Die in Social Media-Plattformen eingestellten Daten sind ihrem Zweck nach für andere Nutzer dieser Plattformen bestimmt und nicht für Dritte, die mit diesen Daten ohne Wissen der Nutzer verfahren.

Im zweiten Fall (§ 30a Abs. 1 Nr. 2 BDSG) ist die Datennutzung erlaubt, wenn diese Daten aus allgemein zugänglichen Quellen entnommen werden können, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Verwendung der Daten offensichtlich überwiegt. Allgemein zugängliche Quellen sind im Bereich des Internets solche, welche sich von einem individuell nicht bestimmbaren Personenkreis – also von jedermann – aufrufen lassen.[16] Sind sie dagegen nur für einen bestimmten Personenkreis abrufbar (wie z.B. geschützte Benutzerprofile bei *Facebook*), so können sie nicht mehr als allgemein zugänglich qualifiziert werden.

Nach diesen Grundsätzen dürften fast alle von Monitoring-Anbietern verwendeten Quellen „allgemein zugänglich" sein, da sowohl die meisten Blogs und Foren als auch *Twitter*-Streams und *Facebook*-Seiten unproblematisch ohne technische Zugangshürden aufgerufen werden können. Ohne Belang ist es dabei auch, dass die Daten z.B. bei *Facebook* über die API und nicht über die Website erhoben werden, denn das Gesetz stellt lediglich darauf ab, dass die Daten allgemein zugänglich sind – nicht dass die Daten auch über allgemein zugängliche Quellen erhoben werden.[17] Lediglich Daten aus geschlossenen Foren, welche vom Monitoring-Anbieter nur mittels eines Passworts vom Forenbetreiber indexiert werden können, fehlt diese Eigenschaft der allgemeinen Zugänglichkeit. Eine Verwendung ist in diesem Fall rechtswidrig.

Stammen die Daten aus einer allgemein zugänglichen Quelle, ist in einem zweiten Schritt ebenfalls eine Interessenabwägung vorzunehmen.[18] Diese ist allerdings dadurch abgeschwächt, dass die Datenverwendung nur dann untersagt wird, wenn ein entgegenstehendes Interesse des Betroffenen offensichtlich ist

12 *Simitis*, in: Simitis (o. Fußn. 5), § 4a Rdnr. 36 f.; *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, BDSG § 4a Rdnr. 6; *Körner-Dammann*, NJW 1992, 729, 730; *Piltz*, CR 2011, 657, 659.
13 *Ehrmann*, in: Simitis (o. Fußn. 5), § 30a Rdnr. 137.
14 *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 29 Rdnr. 10.
15 *Gola/Schomerus* (o. Fußn. 14), § 1 Rdnr. 7.
16 *Gola/Schomerus* (o. Fußn. 14), § 28 Rdnr. 33a; *Simitis* (o. Fußn. 12), § 28 Rdnr. 151.
17 *Simitis* (o. Fußn. 12), § 28 Rdnr. 159.
18 *Simitis* (o. Fußn. 12), § 28 Rdnr. 162.

und dieses gegenüber dem Interesse der verantwortlichen Stelle offensichtlich überwiegt.[19] Im Bereich der Markt- und Meinungsforschung wird dabei angenommen, dass wegen der Schaffung des speziellen § 30a BDSG schutzwürdige Interessen des Betroffenen, welche offensichtlich überwiegen, regelmäßig nicht gegeben sind.[20]

Ist die Erhebung von Daten nach den obenstehenden Ausführungen zulässig, so dürfen diese Daten auch gespeichert und verarbeitet werden (indizierende Wirkung der Erhebung[21]), wobei allerdings immer das Gebot der frühestmöglichen Anonymisierung zu beachten ist. Diese schreibt § 30a Abs. 3 BDSG zum Schutz der gespeicherten Daten vor. Für eine Anonymisierung reicht es nicht immer aus, die Einzelangaben wie Name, Anschrift etc. zu löschen. Vielmehr müssen auch solche Angaben gelöscht werden, aus denen Rückschlüsse auf den Betroffenen gezogen werden können.[22] Ab dem Zeitpunkt der Anonymisierung unterfallen die Daten schließlich nicht mehr dem BDSG und können daher auch frei an die Auftraggeber übermittelt werden.[23] Eine nicht-anonymisierte Übermittlung ist nach § 30a BDSG nicht erlaubt. Hierfür müssen bereits bei der Erhebung die strengeren Regelungen des § 29 BDSG beachtet werden.

d) Grundsatz der Direkterhebung

Ist eine Datenerhebung nach dem oben Gesagten auch ohne Einwilligung des Betroffenen möglich, stellt sich jedoch die weitere Frage, ob der Datenerhebung möglicherweise der Grundsatz der Direkterhebung nach § 4 Abs. 2 BDSG entgegensteht.[24] Danach müssen Daten grundsätzlich mit Kenntnis oder Mitwirkung des Betroffenen erhoben werden, es sei denn, es greift ein Ausnahmetatbestand ein.[25] Nach § 4 Abs. 2 Satz 2 Nr. 1 BDSG ist eine Datenerhebung ohne Mitwirkung des Betroffenen dann möglich, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt. Hierunter fallen nach allgemeiner Ansicht auch die Vorschriften, die eine Datenerhebung aus öffentlich zugänglichen Quellen erlauben, da ansonsten deren Anwendungsbereich weitestgehend aufgehoben wäre.[26] Somit ist die Datenerhebung, soweit sie nach § 30a Abs. 1 Nr. 2 BDSG möglich ist, auch ohne die Mitwirkung des Betroffenen erlaubt.

3. Keine Auftragsdatenverarbeitung

Anzumerken bleibt, dass das Monitoring regelmäßig keine Auftragsdatenverarbeitung nach § 11 Abs. 1 BDSG darstellt. Eine solche liegt nur dann vor, wenn der Auftraggeber nicht nur rechtlich, sondern prinzipiell auch tatsächlich in der Lage ist, dem Auftragnehmer jeden Arbeitsschritt vorzuschreiben und die Durchführung des Datenumgangs zu kontrollieren.[27] Da Auftraggeber von Monitoring-Anbietern in der Regel keinen detaillierten Einfluss darauf nehmen können, welche Daten erhoben, verarbeitet und gespeichert werden, fehlt es an einem Auftragsverhältnis i.S.d. § 11 BDSG.

4. Zwischenergebnis

Zusammenfassend lässt sich feststellen, dass die Tätigkeit der Monitoring-Anbieter, soweit sie zum Zwecke der Markt- und Meinungsforschung und unter Einhaltung des § 30a BDSG erfolgt, datenschutzrechtlich unbedenklich ist. Unzulässig ist lediglich eine werbliche Nutzung der gewonnenen personenbezogen Daten bzw. eine nicht-anonymisierte Übermittlung an die Kunden des Monitoring-Anbieters. Hierzu müssen bereits bei der Datenerhebung die strengeren Vorgaben des § 29 BDSG beachtet werden.

III. Urheberrecht

Im Bereich des Social Media Monitoring spielt auch das Urheberrecht eine entscheidende Rolle. Da die Anbieter große Mengen an nutzergenerierten Inhalten herunterladen, um sie in ihren eigenen Datenbanken zu speichern, stellt sich die Frage nach der urheberrechtlichen Zulässigkeit dieses Vorgehens.

1. Anwendbarkeit des Urheberrechts

Bei der Frage der Anwendbarkeit des UrhG gehen die herrschende Lehre und die Rechtsprechung vom Schutzlandprinzip aus.[28] Dieses besagt, dass für Fragen des geistigen Eigentums das Recht desjenigen Staats anzuwenden ist, für dessen Gebiet der Schutz beansprucht wird.[29] Monitoring-Anbieter, welche sich in Deutschland rechtmäßig verhalten wollen, müssen das deutsche Urheberrecht daher beachten, wenn sie eine Vervielfältigungshandlung auf deutschem Boden vornehmen (z.B. über einen in Deutschland stehenden Server) oder Werke (auch) in Deutschland öffentlich zugänglich machen.[30]

2. Urheberrechtlicher Schutz für nutzergenerierte Inhalte

Urheberrechtlichen Schutz genießen grundsätzlich nur persönliche geistige Schöpfungen (Werke) der Literatur, Wissenschaft oder Kunst (vgl. §§ 1, 2 UrhG). Im Bereich des Social Media Monitoring ist besonders die Kategorie der Sprachwerke von Bedeutung, da die Monitoring-Anbieter derzeit lediglich Texte von den Plattformen verarbeiten und speichern.

Ein geschütztes Sprachwerk liegt immer dann vor, wenn es eine gewisse „Schöpfungshöhe" erreicht, sich also von dem Durchschnitt, vom Alltäglichen und rein Handwerklichen abhebt. Dabei schützt das Urheberrecht allerdings nicht nur literarische Meisterwerke, sondern auch Werke mit geringer Individualität – die sog. kleine Münze.[31]

Texte tauchen im Social Web als kurze Sätze auf *Twitter* („Tweets" mit max. 140 Zeichen), längere Nachrichten auf *Facebook* oder auch als umfangreiche Abhandlungen in Blogs und Foren auf. Ob sie dabei urheberrechtlichen Schutz genießen, ist keine Frage der Länge. So können kurze kreative Tweets die erforderliche Schöpfungshöhe erreichen,[32] während einem langen, aber rein beschreibenden Blogbeitrag eben diese fehlt. Zudem kann auch bereits ein kleiner Teil eines Sprachwerks urheberrechtlichen Schutz genießen, wenn dieser seinerseits die erforderliche Schöpfungshöhe erreicht.[33]

Letztlich kann die Frage nach der Schutzfähigkeit nur im jeweiligen Einzelfall bestimmt werden. Die Formel „je banaler ein Beitrag, desto weniger wahrscheinlich ist urheberrechtlicher Schutz"[34] kann dabei nur eine grobe Richtschnur sein – erforderlich ist vielmehr eine genaue Analyse des Texts und des Kontexts, in dem er steht.[35]

---

19 *Gola/Schomerus* (o. Fußn. 14), § 29 Rdnr. 19.
20 *Ehrmann* (o. Fußn. 13), § 30a Rdnr. 122.
21 *Ehrmann* (o. Fußn. 13), § 30a Rdnr. 124.
22 *Gola/Schomerus* (o. Fußn. 14), § 30a Rdnr. 6.
23 *Ehrmann* (o. Fußn. 13), § 30 Rdnr. 75 ff.
24 *Gola/Schomerus* (o. Fußn. 14), § 4 Rdnr. 19.
25 *Sokol*, in: Simitis (o. Fußn. 5), § 4 Rdnr. 20.
26 *Gola/Schomerus* (o. Fußn. 14), § 4 Rdnr. 24; *Ehrmann* (o. Fußn. 13), § 30a Rdnr. 112 ff.
27 *Petri*, in: Simitis (o. Fußn. 5), § 11 Rdnr. 20.
28 *Walter*, in: Loewenheim, Hdb. des Urheberrechts, 2. Aufl. 2010, § 58 Rdnr. 24.
29 *v. Welser*, in: Wandtke/Bullinger, Urheberrecht, 3. Aufl. 2009, Vor §§ 120 ff. Rdnr. 4.
30 *Dreier*, in: Dreier/Schulze, Urheberrechtsgesetz, 3. Aufl. 2008, Vor §§ 120 ff. Rdnr. 33 u. 40 ff.; vgl. auch *Hoeren* (o. Fußn. 9), S. 117.
31 *Nordemann*, in: Loewenheim (o. Fußn. 28), § 6 Rdnr. 17.
32 *Krieg*, K&R 2010, 73, 75.
33 *EuGH* ZUM 2009, 945.
34 *Reinemann/Remmertz*, ZUM 2012, 216, 217.
35 *Nordemann* (o. Fußn. 31), § 6 Rdnr. 17.

3. Eingriff in die Verwertungsrechte

Da nunmehr feststeht, dass Texte im Social Web durchaus urheberrechtlichen Schutz genießen können, ist weiter zu untersuchen, ob Monitoring-Anbieter diese Rechte verletzen, indem sie die Texte in ihre Datenbanken übernehmen und an ihre Kunden weiterreichen.

Die Übernahme von urheberrechtlich geschützten Texten in die Datenbank greift zunächst in das Vervielfältigungsrecht nach § 16 UrhG ein, da jede körperliche Festlegung des Werks – also auch eine Speicherung auf Datenträgern[36] – eine Vervielfältigung darstellt. Unerheblich ist dabei, dass die Texte nicht unmittelbar wahrnehmbar sind, da sie kodiert gespeichert werden. Es genügt eine mittelbare Wahrnehmbarkeit, wenn sich aus der kodierten Fassung über mehrere Zwischenschritte wieder der Originaltext herstellen lässt.[37]

Werden die geschützten und in die Datenbank kopierten Texte später vom Monitoring-Anbieter über das Internet – also unkörperlich – an Kunden übermittelt, dürfte regelmäßig das Recht der öffentlichen Zugänglichmachung nach § 19a UrhG verletzt sein. Die erforderliche Öffentlichkeit besteht nach der Definition des § 15 Abs. 3 Satz 2 UrhG dann, wenn zwischen den Personen keine persönliche Beziehung besteht. Eine rein vertragliche Beziehung, wie sie zwischen Monitoring-Anbieter und Auftraggeber der Regelfall ist, begründet noch keine solche persönliche Bindung.[38]

4. Einschränkung der Urheberrechte

Da Urheberrechte allerdings keine uneingeschränkten Ausschließlichkeitsrechte sind, sondern gem. Art. 14 GG der Sozialbindung unterliegen, existieren in §§ 44a ff. UrhG verschiedene Schrankenregelungen, welche die Nutzung von Werken trotz grundsätzlich bestehendem Urheberrechtsschutz erlauben.[39] Im Bereich von Texten aus dem Social Web kommt hier lediglich die Zitierfreiheit gem. § 51 UrhG als relevante Schrankenregelung in Betracht. Danach ist die Vervielfältigung, Verbreitung und öffentliche Wiedergabe eines Werks zum Zwecke des Zitats zulässig. Ein Zitat darf dabei nicht für sich alleine stehen, sondern muss eine Belegfunktion aufweisen, d.h. es muss eine innere Verbindung zwischen dem verwendeten fremden Werk und den eigenen Gedanken des Zitierenden hergestellt werden.[40] Kommt dem Werk ohne das Zitat keinerlei eigenständige Existenz zu, so fehlt es an dem erforderlichen Zitatzweck.[41]

Geht man von diesen Grundsätzen aus, ist die Verwendung von geschützten Texten durch Monitoring-Anbieter nicht von der Zitierfreiheit gedeckt. Die Texte in den Datenbanken der Anbieter dienen nicht als Belegstelle oder Erörterungsgrundlage für selbständige Ausführungen des Zitierenden. Eine Auseinandersetzung mit den Inhalten der Texte findet nicht statt. Vielmehr soll die Katalogisierung in den Datenbanken lediglich der besseren Auffindbarkeit und Zugänglichmachung dienen.

5. Einräumung von Nutzungsrechten

Eine Verletzung von Verwertungsrechten scheidet ferner aus, wenn dem Handelnden das Recht eingeräumt wurde, das Werk in einer bestimmten Art und Weise zu nutzen (§ 31 Abs. 1 UrhG). Dies kann ausdrücklich oder auch konkludent durch schlüssiges Handeln erfolgen. Allerdings kann man eine solche – ausdrückliche oder konkludente – Rechteeinräumung seitens der Nutzer von Social Media-Plattformen wohl nicht annehmen, da diese sich kaum Gedanken darüber machen, dass Monitoring-Anbieter ihre Texte verwenden und daher auch keinen rechtlichen Bindungswillen bilden können.

6. Schlichte Einwilligung in die Nutzung

An der Rechtswidrigkeit des Eingriffs in die Verwertungsrechte der Urheber kann es allerdings auch dann fehlen, wenn der Urheber in diese Verwertung (schlicht) eingewilligt hat,[42] was wiederum ausdrücklich oder konkludent erfolgen kann. Der *BGH* hat sich in der vielbeachteten Entscheidung „Vorschaubilder I"[43] ausführlich mit der schlichten Einwilligung befasst. Er kommt darin zu dem Ergebnis, dass das bloße Einstellen von Inhalten ins Internet, ohne von bestehenden Schutzmöglichkeiten (z.B. dem Eintrag in eine robots.txt) Gebrauch zu machen, eine Einwilligung in die Verwendung der Inhalte durch Suchmaschinen darstellt. Grund hierfür sei, dass die Darstellung von urheberrechtlich geschützten Inhalten durch Suchmaschinen im Internet üblich sei und der Urheber daher mit einer solchen üblichen Nutzungshandlung rechnen müsse. Wolle er dies nicht, so könne er sich durch technische Maßnahmen dagegen wehren. Fraglich ist, ob diese Wertungen auch auf die Tätigkeit der Monitoring-Anbieter übertragbar sind. Dies ist in zweierlei Hinsicht zweifelhaft.

Zum einen existieren bei weitem nicht für alle Benutzer von Social Media-Plattformen technische Möglichkeiten, den „Download" von Inhalten durch Monitoring-Anbieter zu verhindern. Mag dies bei selbst gehosteten Blogs über die robots.txt noch möglich sein, gestaltet sich die Verhinderung bereits bei Foren schwierig, da hier grundsätzlich lediglich der Forenbetreiber technische Maßnahmen ergreifen kann. In sozialen Netzwerken wie *Facebook* oder auch beim Microblogging-Dienst *Twitter* existiert dagegen überhaupt keine Möglichkeit, den Zugriff durch Monitoring-Anbieter zu unterbinden. Postet ein User einen Kommentar auf einer *Facebook*-Seite, so richtet sich die öffentliche Sichtbarkeit dieses Beitrags lediglich nach den Einstellungen des Seitenbetreibers – der User hat hierauf keinen Einfluss.[44]

Zum anderen dürfte die Tätigkeit der Monitoring-Anbieter nicht in dem Maße üblich sein, dass jeder Internetnutzer mit der Indexierung und Katalogisierung rechnen muss. Vielmehr findet die Arbeit von Monitoring-Anbietern – anders als die Tätigkeit von Suchmaschinen – üblicherweise für die Nutzer unsichtbar und daher unbemerkt statt. Während jeder Internetnutzer inzwischen über die Möglichkeiten der Suchmaschinen Kenntnis hat und im Zweifelsfall eigene Inhalte auch schnell selbst „googlen" kann, fehlt dieses Bewusstsein hinsichtlich Monitoring-Anbietern bei einem Großteil der Nutzer von Social Media-Angeboten. Ein durchschnittlicher Nutzer mag sich möglicherweise noch bewusst sein, dass *Facebook* die Inhalte selbst in Datenbanken ablegt und evtl. auch Suchmaschinen auf diese Inhalte Zugriff haben. Er dürfte allerdings wohl kaum damit rechnen, dass seine Inhalte auch durch einen Monitoring-Anbieter indexiert, katalogisiert und anschließend an dessen Kunden weitergegeben werden.

Wie dargestellt, ist eine schlichte konkludente Einwilligung in die Urheberrechtsverletzung durch Monitoring-Anbieter nicht anzunehmen. Letztlich ist diese Frage allerdings noch nicht höchstrichterlich entschieden, sodass insoweit noch eine erhebliche Rechtsunsicherheit besteht.

---

36 *Schulze*, in: Dreier/Schulze (o. Fußn. 30), § 16 Rdnr. 7.
37 *Heerma*, in: Wandtke/Bullinger (o. Fußn. 29), § 16 Rdnr. 2.
38 *Heerma* (o. Fußn. 37), § 15 Rdnr. 18.
39 *Lüft*, in: Wandtke/Bullinger (o. Fußn. 29), Vor §§ 44a ff. Rdnr. 1.
40 *BGH* NJW 2010, 2731; *BGH* MMR 2008, 536, 539 – TV Total m.w.Nw.
41 *Wiebe*, in: Spindler/Schuster (o. Fußn. 12), § 51 Rdnr. 2; *BGH* NJW 1986, 131, 132 – Geistchristentum.
42 *Wandtke/Grunert*, in: Wandtke/Bullinger (o. Fußn. 29), § 31 Rdnr. 37.
43 *BGH* MMR 2010, 475 m. Anm. *Rössel*.
44 Abrufbar unter: https://www.facebook.com/help/?faq=241358369283005#Wer-kann-was-auf-einer-Facebook-Seite-sehen?

7. Auswirkungen auf die Praxis der Monitoring-Anbieter

Da, wie oben aufgezeigt, der urheberrechtliche Schutz von Beiträgen im Social Web von einer Betrachtung des jeweiligen Einzelfalls abhängt, sich pauschale Aussagen („Einzelne Tweets sind nicht geschützt"[45]) verbieten und eine ausnahmsweise rechtmäßige Nutzung von geschützten Inhalten ausscheidet, stellt das Urheberrecht eine große Hürde für die Dienstleistungen der Monitoring-Anbieter dar. Nach der hier vertretenen Auffassung können Monitoring-Anbieter lediglich solche Texte in ihre Datenbanken aufnehmen und an Kunden weiterreichen, welche nicht die erforderliche Schöpfungshöhe erreichen und damit nicht dem Schutz des UrhG unterfallen. Die zur Feststellung der Schöpfungshöhe notwendige händische Kontrolle der Texte im Einzelfall dürfte allerdings für Monitoring-Anbieter kaum leistbar sein.

IV. Ausblick

Wie die Untersuchung gezeigt hat, stellt das Datenschutzrecht für Monitoring-Anbieter mit § 30a BDSG eine taugliche Erlaubnisnorm zur Erhebung und Verarbeitung von personenbezogenen Daten aus allgemein zugänglichen Quellen bereit. Sie können ihre Dienstleistungen damit beinahe ungestört vom Datenschutzrecht erbringen. Größere Schwierigkeiten bereitet dagegen das Urheberrecht, wenn urheberrechtlich geschützte Texte in die Datenbanken der Monitoring-Anbieter übernommen und an Kunden weitergereicht werden. Da diese Tätigkeit weder von der Zitierfreiheit noch von einer schlichten Einwilligung der Urheber gedeckt ist, dürfen diese Texte von den Monitoring-Anbietern nicht verwendet werden. Als Alternative zum gänzlichen Verzicht auf urheberrechtlich geschütztes Material wäre es allenfalls möglich, in die Datenbank lediglich Deep Links zu den Originalquellen aufzunehmen, denn dies stellt nach der ständigen Rechtsprechung keine urheberrechtlich relevante Verletzungshandlung dar.[46]

Christian Solmecke, LL.M.
ist Rechtsanwalt und Partner der Kanzlei Wilde Beuger Solmecke in Köln.

Jakob Wahlers, Dipl.-Jur.
ist Rechtsreferendar im Landgerichtsbezirk Aachen und im Rahmen seiner Wahlstation bei Wilde Beuger Solmecke tätig.

45 So aber *Ulbricht*, abrufbar unter: http://www.rechtzweinull.de/index.php?/archives/94-Twitter-und-Recht-Sind-Tweets-urheberrechtlich-geschuetzt.html.
46 *Dreier* (o. Fußn. 30), § 19a Rdnr. 6; *BGH* MMR 2003, 719 m. Anm. *Wiebe*.