8 Datenschutz im Social Web

8.1 Die Grundlagen

Die zentralen Vorschriften für den Datenschutz im Social Web finden sich im → Telemediengesetz (TMG). Dort wird der Schutz der anfallenden → personenbezogenen Daten bei der Nutzung von Telemediendiensten gegenüber dem Diensteanbieter geregelt.

§ 13 TMG legt in Absatz 1 fest, dass der Anbieter eines (Internet-)Dienstes seine Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung **personenbezogener Daten** in allgemein verständlicher Form informieren muss, sofern eine solche Unterrichtung nicht bereits vorher erfolgt ist.

Wie das → Bundesdatenschutzgesetz (BDSG), stellt das für Internetdienste vorrangige Telemediengesetz also auf den Begriff der „personenbezogenen Daten" ab. Nur wenn personenbezogene Daten verarbeitet werden, greifen überhaupt die Datenschutzvorgaben des Telemediengesetzes bzw. des Bundesdatenschutzgesetzes ein.

Der § 13 TMG enthält für den Betreiber eines Telemediendienstes außerdem die Pflicht, den Nutzer auf sein Widerrufsrecht hinzuweisen (Abs. 3), die Pflicht zur Anzeige der Weitervermittlung von Daten (Abs. 5) sowie auf Nachfrage die Auskunftserteilung über die zu seiner Person gespeicherten Daten (Abs. 7).

Betreiber einer entsprechenden Internetpräsenz sollten demnach in jedem Fall eine leicht auffindbare → Datenschutzerklärung vorhalten, die gemäß § 13 TMG über die Datenerhebung informiert.

8.1.1 Personenbezogene Daten: Dreh- und Angelpunkt des Schutzes

Personenbezogene Daten sind nach der Definition des § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)". Diese Einzelangaben werden sehr weit gefasst.

- So fallen unter „persönliche Verhältnisse" Angaben zu dem Betroffenen selbst, seine Identifizierung und Charakterisierung (z. B. Name, Anschrift, Familienstand, Geburtsdatum, Staatsangehörigkeit, Konfession, Beruf, Erscheinungsbild, Eigenschaften, Aussehen, Gesundheitszustand, Überzeugungen).
- Die „sachlichen Verhältnisse" betreffen Angaben über einen auf den Betroffenen beziehbaren Sachverhalt, wie z. B. seinen Grundbesitz.

Immer dann, wenn entsprechende Daten in oder über die Sozialen Medien verarbeitet werden, sind vom Diensteanbieter die Vorgaben des → Telemediengesetzes zu beachten.

Auch im Telemedienrecht gilt der Grundsatz des → Verbots mit Erlaubnisvorbehalt (§ 12 TMG). Das bedeutet, dass man personenbezogene Daten nur verwenden darf, wenn dies gesetzlich ausdrücklich erlaubt wird oder dazu eine Einwilligung des jeweils betroffenen Nutzers vorliegt.

Wenn also personenbezogene Daten der Social Web Nutzer gesammelt oder verwendet werden, sollte grundsätzlich sichergestellt werden, dass die konkrete Datenverwendung

- entweder ausdrücklich durch eine gesetzliche Vorschrift für zulässig erklärt wird oder
- der Nutzer vor der Datenerhebung oder -verwendung entsprechend § 13 TMG umfassend aufgeklärt wird und seine ausdrückliche Zustimmung (Opt-in) dazu erklärt hat.

8.1.2 Die Einwilligung des Nutzers

§ 13 TMG schreibt vor, Nutzer über die Datenerhebung mit einer leicht auffindbaren → Datenschutzerklärung zu informieren. Bei der Erhebung oder Verarbeitung personenbezogener Daten kann dazu die Verpflichtung hinzukommen, eine Einwilligung des jeweils betroffenen Nutzers einzuholen. Ob neben der Datenschutzerklärung eine zusätzliche Einwilligung erforderlich ist, hängt davon ab, ob und wie personenbezogene Daten erhoben, verarbeitet oder an Dritte weitergegeben werden. Ob besondere Funktionen in den Sozialen Medien, wie z. B. der Facebook Like Button, eine solche Einwilligung erfordern und wie dies in der Praxis umgesetzt werden kann, wird in diesem Kapitel dargestellt.

Eine datenschutzrechtliche Einwilligung erfordert in der Regel eine aktive Zustimmungserklärung des Betroffenen (→ Opt-in). Häufig wird dies so realisiert: Der Nutzer muss der Erklärung des Anbieters zur Datenerhebung und -verarbeitung durch das Setzen eines Häkchens in einer Checkbox zustimmen. Dieses Verfahren genügt den datenschutzrechtlichen Anforderungen.

Ist eine Einwilligung nötig, muss der Diensteanbieter auch sicherstellen:

- dass die Einwilligung protokolliert wird (§ 13 Nr. 2 TMG),
- der Inhalt der Einwilligung für den Nutzer jederzeit abrufbar ist (Nr. 3) und
- er seine Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen kann (Nr. 4).

Über diese Widerrufsmöglichkeit muss der Nutzer in der → Datenschutzerklärung informiert werden.

TIPP: Mit einer Einwilligung sind Sie auf der sicheren Seite

So gut wie jede Art der Datenerhebung oder -verarbeitung ist zulässig, wenn hierzu eine entsprechende Einwilligung des Nutzers vorliegt.

8.2 Social Media Monitoring: das „Durchsuchen“ des Social Web

Auch in Deutschland haben viele Unternehmen das große Potenzial des Sozialen Internets erkannt. Bevor sie jedoch selbst aktiv werden, nähern sich Unternehmen dem Phänomen häufig, indem sie bei den Dialogen und der Meinungsbildung zuhören und sie beobachten.

Social Media Monitoring heißt hier das aktuelle Zauberwort. Es symbolisiert als ersten Schritt einer Social Media Strategie das Beobachten, Filtern und Analysieren von nutzergenerierten Inhalten (sog. User Generated Content) auf Social Media Plattformen, wie z. B. Facebook, Twitter, YouTube etc. Monitoring wird daneben im Reputations- und Krisenmanagement und zur Markt- und Wettbewerbsanalyse eingesetzt. Tatsächlich bietet die systematische Recherche und Auswertung vieler Informationen im Social Web für Unternehmen interessante und sehr wichtige Erkenntnisse. Zukünftig wird das Beobachten des Social Web daher auch für das Customer Relationship Management (CRM) sowie für die Marktforschung und das Produkt- und Innovationsmanagement an Bedeutung gewinnen. Insofern ist eine entsprechende Aus- und Bewertung der Informationen im Social Web auch für neue Geschäftsmodelle eine interessante Grundlage.

Wie eine Studie des Fraunhofer-Instituts[1] anschaulich zeigt, wird Social Media Monitoring derzeit vor allem von der Kommunikations- und/oder Marketingabteilung eines Unternehmens angestoßen bzw. betrieben.

TIPP: Wie Monitoring funktioniert

Um herauszufinden, was in den Sozialen Medien über sie geschrieben wird, können Unternehmen entweder die im Internet zugänglichen Werkzeuge[2] nutzen oder aber einen der professionellen Anbieter mit dem Monitoring über individualisierte Suchroutinen beauftragen. Letzteres ist ab einem gewissen Komplexitätsgrad hinsichtlich der Konfiguration der Suchwörter, der Zahl der Quellen und spezifischer Zielsetzung sicherlich ratsam.

[1] Kasper/Dausinger/Kett/Renner, Marktstudie Social Media Monitoring Tools – IT-Lösungen zur Beobachtung und Analyse unternehmensstrategisch relevanter Informationen im Internet, Fraunhofer Verlag 2010.

[2] Siehe Übersicht unter http://www.prdaily.com/Main/Articles/4ef9fcd6-224c-403b-927c-1317a4d35634.aspx.

8.2.1 Datenschutz: zentrales Problem des Social Media Monitoring

Eine zielgerichtete Erhebung von Daten aus Facebook, XING & Co.steht allerdings in einem unausweichlichen Spannungsverhältnis zum Thema Datenschutz. Für Unternehmen sollte die Einhaltung von datenschutzrechtlichen Vorgaben ein wichtiger Aspekt bei der Auswahl des Dienstleisters im Bereich Social Media Monitoring sein. Auch beim Einsatz eigener Monitoring-Werkzeuge sollten Unternehmen sich der datenschutzrechtlichen Grenzen bewusst sein.

Neben allgemeineren datenschutzrechtlichen Einflüssen wird — je nach Ausrichtung der Monitoringroutinen — auch das Thema Arbeitnehmerdatenschutz beim Social Media Monitoring relevant werden. Oft wird ein Unternehmen bei entsprechenden Suchroutinen nach der eigenen Marke auch auf Informationen und Aussagen der eigenen Mitarbeiter stoßen. Auch wegen der mittlerweile in die nächste Legislaturperiode verschobenen gesetzlichen Neuregelung des Arbeitnehmerdatenschutzrechts kommen Monitoring betreibende Unternehmen, die nicht blindlings in Probleme mit Datenschutzbehörden hineinlaufen wollen, an einer rechtlichen Risikoanalyse nicht vorbei. Auch wenn in diesem relativ neuen Themenfeld rechtlich Einiges noch nicht abschließend geklärt ist, werden hier die Grenzen nachgezeichnet und Risiken erläutert, aber auch zulässige Gestaltungen dargestellt.

8.2.2 Ist Monitoring überhaupt zulässig?

1. Datenschutzrechtliche Grundlagen

Nach § 4 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung **personenbezogener Daten** nur zulässig, wenn der Betroffene eingewilligt hat oder eine Rechtsvorschrift die jeweilige Datenverwendung auch ohne Einwilligung zulässt. Das gilt aber nur bei → personenbezogenen Daten (siehe Kapitel 8.1.1). Soweit also keine personenbezogenen Daten i. S. des § 3 Abs. 1 BDSG betroffen sind, d. h. keine Informationen, die einer bestimmten oder bestimmbaren natürlichen Person zuzuordnen sind, greift das → Bundesdatenschutzgesetz überhaupt nicht ein. Die Diskussion im Zusam-

menhang mit Google Analytics und die datenschutzrechtliche Relevanz von IP-Adressen zeigt aber bereits, dass die Frage nach dem Personenbezug von Daten oft nur schwierig zu beantworten ist.

Das bei personenbezogenen Daten geltende → Verbot mit Erlaubnisvorbehalt bezieht sich auf jede Stufe der Verwendung personenbezogener Daten. Danach muss beim Social Media Monitoring nicht nur bei der Erhebung personenbezogener Daten, sondern auch bei der Speicherung oder einer weitergehenden Datenverarbeitung (d. h. Auswertung, Aggregation etc.) die Zulässigkeit geprüft werden.

Nachdem der jeweils Betroffene, dessen Daten erhoben werden, in aller Regel nicht in die Erhebung durch unbekannte Dritte (sprich dem „monitorenden" Unternehmen) eingewilligt hat, bleiben als legitimierende Rechtsvorschriften nur die weiteren Regelungen des → Bundesdatenschutzgesetzes (BDSG).

2. Datenerhebung aus öffentlich zugänglichen Quellen (§ 28 Abs. 1 Nr. 3 BDSG)

Eine ganz zentrale Vorschrift ist deshalb § 28 Abs. 1 Nr. 3 BDSG (für Monitoring-Anbieter entsprechend § 29 Abs. 1 Satz 1 Nr. 2 BDSG). Danach dürfen Daten, die öffentlich zugänglich sind, auch per Social Media Monitoring erhoben werden. Dabei darf aber das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder der Nutzung das berechtigte Interesse der verantwortlichen Stelle nicht offensichtlich überwiegen. Diese Vorschrift geht von dem Grundsatz aus, dass es demjenigen, der sich aus allgemein zugänglichen Quellen unterrichten darf, auch grundsätzlich gestattet sein muss, die dort zugänglichen Daten zu speichern. Öffentlich zugänglich sind juristisch gesprochen alle Informationsquellen, „die sich sowohl ihrer technischen Ausgestaltung als auch ihrer Zielsetzung nach dazu eignen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln" (Simitis in: Simitis, Hrsg., BDSG § 28 Rn. 189). Damit sind Informationen aus dem Internet immer dann als öffentlich zugänglich zu werten, wenn sie zulässigerweise als für jedermann zugängliche Daten im WorldWideWeb verfügbar gemacht worden sind.

- Informationen, die nur unter gewissen Einschränkungen verfügbar sind, z. B. weil sie nur von angemeldeten Nutzern eines Sozialen Netzwerkes eingesehen werden können, sind dagegen nicht als für jedermann, und damit nicht als öffentlich zugänglich zu werten. In solchen Fällen kann zwar nicht § 28 Abs. 1 Nr. 3 BDSG herangezogen werden, unter Umständen aber andere Normen des BDSG als gesetzliche Rechtfertigung.
- Wenn aber nur öffentlich zugängliche Informationen die Datenbasis des Social Media Monitoring sind, ist die Erhebung zulässig, wenn der Verarbeitung nicht offensichtliche Interessen des Betroffenen entgegenstehen. Das hängt letztlich von der Sensibilität der Daten ab.
- Diese Vorschrift ermöglicht bei entsprechender Konfiguration der Monitoring Tools also bereits eine Beschränkung datenschutzrechtlicher Risiken.

3. Anonymisierung und Pseudonymisierung von Daten

Gefragt nach der datenschutzrechtlichen Zulässigkeit, erwidern Anbieter von Monitoring Tools gern, diese Vorgaben seien nicht betroffen, da ja keine persönlichen Informationen wie z. B. Namen erhoben werden würden. Diese Argumentation greift aber oft zu kurz, weil es bei den vom BDSG geschützten Daten um personenbezogene Daten i. S. des § 3 BDSG, also um deutlich mehr als nur Namen, Anschrift o. Ä., geht. Daher wird man bei der datenschutzrechtlichen Beurteilung genauer hinschauen müssen. Nachdem aber tatsächlich nur Daten mit einem entsprechenden Personenbezug i. S. des § 3 Abs. 1 BDSG geschützt sind, ist es möglich, durch eine Anonymisierung oder Pseudonymisierung Daten so zu modifizieren, dass die jeweilige Nutzung zulässig ist bzw. wird. Bei der Anonymisierung (§ 3 Abs. 6 BDSG) werden alle Informationen aus den zu speichernden Daten dauerhaft entfernt, die zur Identifizierung der dahinter stehenden Person notwendig sind. Das kann die (Weiter-) Verwertung zulässig machen. Pseudonymisieren (§ 3 Abs. 6a BDSG) hingegen ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Datenschutzkonformes Monitoring ist also grundsätzlich möglich. Beim „Aufsetzen“ eines Monitoring Tools sollte bedacht werden, dass jeder einzelne Monitoring-Schritt den Datenschutzvorgaben entsprechen muss: Angefangen von der Erhebung der Daten über deren notwendige Speicherung und

Verarbeitung bis hin zu einer etwaigen Weitergabe an das beauftragende Unternehmen, muss — soweit personenbezogene Daten verwertet werden — eine gesetzliche Vorschrift aus dem BDSG die Datenverwendung legitimieren.

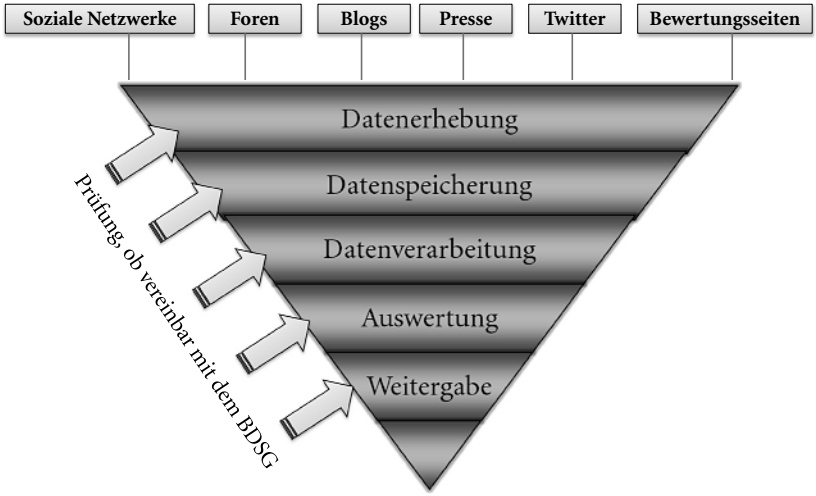

Abb. 3: Datenschutzrecht & Social Media Monitoring

8.2.3 Vertrag über Auftragsdatenverarbeitung: für beide Seiten sinnvoll

Wer einen Dritten mit der Erhebung oder Verarbeitung geschützter Daten beauftragt, bleibt selbst nach § 11 Abs. 1 BDSG für die Einhaltung des Datenschutzrechts verantwortlich. In diesen Fällen (z. B. bei Beauftragung eines Monitoring Anbieters durch ein Unternehmen) liegt es im höchsteigenen Interesse des Auftraggebers, einen Vertrag über eine Auftragsdatenverarbeitung mit den Inhalten des § 11 Abs. 2 BDSG zu schließen, um so für eine Datenschutzkonformität des Monitorings sorgen zu können. Auch für Social Monitoring Anbieter lohnt sich ein solcher Vertrag: Sie können über den Abschluss dieser Verträge das Vertrauen ihrer Kunden gewinnen.