

Dr. Martin Bahr

»Rechtliche Zulässigkeit von Online-Benutzerprofilen – Teil 1

Obgleich die rechtlich einwandfreie Verwendung von Online-Benutzerprofilen ein wichtiges Thema darstellt, ist die Anzahl der leicht verständlichen und nachvollziehbaren juristischen Aufsätze mehr als überschaubar. Diese Lücke schließt Rechtsanwalt Dr. Martin Bahr mit einem zweiteiligen Beitrag. Im vorliegenden ersten Teil werden die Grundlagen erörtert und erklärt. Teil 2 wird sich dann der spannenden Frage widmen, was es zu beachten gilt, wenn solche Daten tatsächlich auch zusammengeführt werden sollen.

Teil A: Die maßgeblichen Gesetze

Der Bereich der Online-Benutzerprofile ist rechtlich nur sehr rudimentär geregelt. Die zwei maßgeblichen Gesetze, in denen sich ansatzweise Bestimmungen finden, sind das Telemediengesetz (TMG) und das Bundesdatenschutzgesetz (BDSG). Die Normen des TMG (§§ 11–15a) gehen den Vorgaben des BDSG grundsätzlich vor, d. h. der Internet-Unternehmer sollte sich primär die Vorschriften des TMG anschauen.

Teil B: Wann ist eine Datenverarbeitung erlaubt?

Das Gesetz erlaubt die Erstellung von Online-Benutzerprofilen in zwei Fällen:

Erstens, wenn es eine gesetzliche Vorschrift gibt, die die Verarbeitung der Daten ausdrücklich erlaubt.

Zweitens, wenn der User der Verarbeitung zuvor zugestimmt hat. Hat der Nutzer eingewilligt, kann der Internet-Unternehmer jeden Sinn und Unsinn mit den Daten machen, den er möchte. Hat er die Zustimmung, so ist jeder „Schweinkram“ erlaubt. Es gibt nur einen Nachteil: In der Praxis ist eine solche Einwilligung kaum wirksam einholbar, denn sowohl an die Art und Weise als auch an den Inhalt werden von der Rechtsprechung nahezu unerfüllbare Voraussetzungen gestellt. Datenschutzrechtliche Einwilligungen können zwar in den AGB platziert werden. Handelt es sich jedoch um inhaltlich weitreichende Bestimmungen, so bedarf es im Zweifel eines ausdrücklichen Hinweises bzw. einer expliziten Zustimmung. Die datenschutz-

rechtlichen Regelungen aller sozialen Netzwerke, die eine weitergehende Nutzung der Daten erlauben, sind daher rechtswidrig.

Gesetzliche Grundlagen

Vorschriften, die ausdrücklich eine Datenverarbeitung erlauben, z. B. § 15 TMG

Vorteil:

Keine Zweifel an der rechtlichen Wirksamkeit der Datenerhebung

Nachteil:

Nur wenige Vorschriften erlauben Datenverarbeitung für Online-Benutzerprofile

Einwilligung

Nutzer stimmt Datenverarbeitung zu

Vorteil:

Großer Anwendungsbereich, da mit Einwilligung jeder „Schweinkram“ erlaubt ist

Nachteil:

Kaum erfüllbare Voraussetzungen an rechtliche Wirksamkeit der Einwilligung

Im Nachfolgenden werden nur die gesetzlichen Grundlagen erörtert. Wer sich für den Bereich der Einwilligung interessiert, kann an anderer Stelle nachlesen.

Teil C: Unterschiedliche Arten von Daten

Das Gesetz differenziert zwischen drei Arten von Daten:

- » anonyme Daten
- » pseudonymisierte Daten
- » Klardaten

DER AUTOR



Dr. Martin Bahr – Die Kanzlei Dr. Bahr (www.dr-bahr.com)

ist auf den Bereich des Rechts der Neuen Medien und den gewerblichen Rechtsschutz (Marken-, Urheber- und Wettbewerbsrecht) spezialisiert. Unter www.suchmaschinen-und-recht.de betreibt sie seit 2005 ein eigenes Themenportal zur rechtlichen Dimension von Suchmaschinen.

Da das TMG unterschiedliche rechtliche Anforderungen an die Datenverarbeitung stellt, bedarf es zunächst der Klärung, was genau unter den einzelnen Begriffen zu verstehen ist.

1. Anonyme Daten:

Bei anonymen Daten handelt es sich um Informationen, die keiner konkreten Person mehr zugeordnet werden können, sondern nur noch abstrakt vorliegen.

Beispiel: Facebook hat aus seinen Benutzerprofilen einen eigenständigen neuen Datensatz erstellt. Darin enthalten ist die Information, dass 54 % der Leute gern Schokoladeneis essen, während nur 33 % der Nutzer Erdbeereis mögen. Es ist nicht mehr rückführbar, welcher der einzelnen User Erdbeere und wer Schokolade bevorzugt.

Anonyme Daten sind somit meistens statistisch relevante Informationen, die über das Verhalten der eigenen Kunden allgemeine Aussagen treffen. Daten über den einzelnen Nutzer erhält der Unternehmer hier nicht.

Nach dem Gesetz handelt es sich auch dann um anonyme Daten, wenn die Informationen zwar theoretisch gesehen noch einem User zugeordnet werden können, jedoch diese Re-Identifizierung nur mit einem unverhältnismäßig großen Aufwand möglich ist (§ 3 Abs. 6 BDSG). Je nach Position werden hier die unterschiedlichsten Ansichten vertreten. Für viele Datenschützer reicht z. B. bereits die theoretische Möglichkeit einer Identifizierung aus. So soll selbst in dem Fall, in dem die Zusatzinformation nur durch Gesetzesverstöße erlangt werden kann, kein unverhältnismäßig großer Aufwand vorliegen.

Für Sie als Internet-Unternehmer bedeutet dies, sobald Ihre anonymen

Daten re-identifizierbar sind, müssen Sie damit rechnen, dass die Datenschützer Ihre Informationen nicht mehr als anonym ansehen, vollkommen unabhängig davon, wie unrealistisch eine solche Ermittlung in der Praxis auch sein mag.

2. Pseudonymisierte Daten:

Pseudonymisierte Daten liegen vor, wenn bestimmte Identifikationsmerkmale in dem jeweiligen Datensatz durch ein Pseudonym ersetzt werden.

Beispiel: Im Datensatz von Facebook ist die Information enthalten, dass der User „Martin Bahr“ von Beruf „Rechtsanwalt“ ist. Facebook entfernt nun den Namen und ersetzt ihn durch ein Pseudonym, z. B. eine Kennzahl wie „00001“. Dieses neue Pseudonym wird nur einmal vergeben. Ein anderer Facebook-Nutzer erhält z. B. die Zahl „00002“.

Sie als Internet-Unternehmen wissen somit nicht mehr, wer sich hinter der Zahl „00001“ verbirgt, da der Name vollständig gelöscht wurde. Sie können jedoch weiterhin alle sonstigen Informationen erkennen.

Beispiel: Es wird gespeichert, dass der Nutzer „00001“ von Beruf „Rechtsanwalt“ ist, Schokoladeneis mag, Erdbeereis hingegen nicht. Auch wird festgehalten, wie lange „00001“ täglich online ist, auf welchen Webseiten er sich aufhält usw.

Wie der Begriff „pseudonymisierte Daten“ schon aussagt, werden hier identifizierbare Merkmale (z. B. Name, Straße und Ort) durch ein Pseudonym ersetzt. Dieses Pseudonym ist jedoch einzigartig (unique), sodass der Unternehmer weiterhin diesem User einzelne Informationen zuordnen kann.

3. Klardaten:

Klardaten sind die Informationen, die zu einer bestimmten natürlichen Person gespeichert werden.

Beispiel: Facebook speichert Vor- und Nachname, Straße, PLZ, Ort und Beruf, also: „Martin Bahr, Mittelweg 41a, 20148 Hamburg, Rechtsanwalt“.

Das BDSG schützt grundsätzlich nur personenbezogene Daten. Das Gesetz definiert personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person“ (§ 3 Abs. 1 BDSG). Zerlegt man diesen Satz in seine Einzelteile, dann müssen drei Voraussetzungen gegeben sein, damit das BDSG überhaupt Anwendung findet:

- » Einzelangaben über persönliche oder sachliche Verhältnisse
- » bestimmt oder bestimmbar
- » natürliche Person

a. Einzelangaben über persönliche oder sachliche Verhältnisse

Die geschützten Daten müssen Informationen über die betreffende Person selbst (= „persönlich“) oder über einen auf sie beziehbar Sachverhalt (= „sachlich“) enthalten.

Beispiel: Angaben über Name, Anschrift, Familienstand, Geburtsdatum, Staatsangehörigkeit, Konfession, Beruf oder Gesundheitszustand sind persönlicher Natur. Angaben über Eigentumsverhältnisse oder Grundbesitz sind sachlicher Natur.

b. Bestimmt oder bestimmbar

Aufgrund der gespeicherten Daten muss eine Person bestimmt bzw. zumindest bestimmbar sein. Bestimmt ist eine Person, wenn sich unmittelbar aus den Daten die Identität der Person ergibt oder herleiten lässt. Bestimmbar ist eine

Person, wenn sie sich unter Zuhilfenahme anderweitiger Daten identifizieren lässt. Ähnlich wie bei der Voraussetzung „unverhältnismäßig großer Aufwand“ bei den anonymen Daten werden auch hier die abenteuerlichsten Ansichten vertreten.

So wird z. B. seit Jahren kontrovers diskutiert, ob IP-Adressen die erforderliche Bestimmbarkeit aufweisen oder nicht. Deutsche Gerichte haben sowohl in die eine als auch in die andere Richtung entschieden. Eine klare Tendenz in der Rechtsprechung ist nicht auszumachen. Auch eine aktuelle Entscheidung des EuGH (Urt. v. 24.11.2011 - Az.: C-70/10) ändert daran nichts, denn es ging dort nur um bereits identifizierte IP-Adressen.

c. Natürliche Person

Das deutsche Datenschutzrecht schützt grundsätzlich nur Informationen über natürliche Personen, also Menschen. Juristische Personen dagegen sind nicht mit umfasst. Das heißt, alle bekannten Personen- und Kapitalgesellschaften unterfallen nicht dem Anwendungsbereich des BDSG. Sie als Internet-Unternehmer können somit Informationen über juristische Personen problemlos verarbeiten. Die Grenzen sind lediglich die allgemeinen Gesetze wie das BGB oder UWG, welche z. B. Geschäfts- und Betriebsgeheimnisse unter einen besonderen Schutz stellen.

Es gilt aber zu beachten, dass die Daten häufig nicht nur Informationen über das Unternehmen enthalten, sondern z. B. auch über den Geschäftsführer, die Gesellschafter, den Vorstand oder den Aufsichtsrat. Ist dies der Fall, so greift das Datenschutzrecht wieder, weil es sich hierbei um gemischte Daten handelt, von denen ein Teil der Informationen eine natürliche Person betrifft. Solche Daten haben jedoch nur einen geringen rechtlichen Schutz, da es sich um sogenannte allgemein zugängliche Daten handelt.

Teil D: Wann sind Online-Benutzerprofile erlaubt?

Nachdem nun geklärt ist, welche Arten von Daten es gibt, stellt sich die Frage, unter welchen gesetzlichen Voraussetzungen eine Erhebung und Verarbeitung erlaubt ist.

1. Anonyme Daten:

Anonyme Daten dürfen Sie als Internet-Unternehmer ohne Wenn und Aber speichern. Das Gesetz stellt hier keinerlei Voraussetzungen oder Einschränkungen auf. Sie können sich also hemmungslos „austoben“.

Bitte beachten Sie aber, dass diese Aussage nur für die anonymen Daten an sich gilt. Wollen Sie hingegen die anonymen Daten erst aus einem Satz Klardaten erzeugen, so gelten für die Verarbeitung der Klardaten diese Aussagen nicht.

Beispiel: Facebook hat einen Datensatz mit Klardaten, also mit Bestandsdaten. Im Datensatz von Facebook ist die Information enthalten, dass der User „Martin Bahr“ von Beruf „Rechtsanwalt“ ist. Facebook entfernt nun den Namen und ersetzt ihn durch ein Pseudonym, z. B. eine Kennzahl wie „00001“. Dieses neue Pseudonym wird nur einmal vergeben. Ein anderer Facebook-Nutzer erhält z. B. die Zahl „00002“.

Anonyme Daten sind somit rechtlich am unproblematischsten. In der Praxis sind sie jedoch häufig die weniger interessanten Informationen, da sie nur Allgemeinaussagen enthalten und nicht auf den einzelnen Nutzer zurückführbar sind. Dies gilt gerade im Zeitalter der personalisierten Werbung des Web 2.0.

2. Pseudonymisierte Daten:

a. Allgemein:

Unter welchen Voraussetzungen pseudonymisierte Daten im Rahmen

von Benutzerprofilen genutzt werden dürfen, regelt § 15 Abs. 3 TMG. Danach darf der Plattform-Betreiber zu „Zwecken der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung“ der Webseiten Nutzungsprofile mit pseudonymisierten Daten erstellen.

Das Gesetz erlaubt somit scheinbar sehr weitreichend die Speicherung pseudonymisierter Daten. Diese Annahme wird jedoch schnell zerstört, wenn man den Gesetzestext weiter liest. Eine Speicherung ist nämlich nur dann erlaubt, wenn der Nutzer dem nicht widersprochen hat. Damit der User überhaupt von der Möglichkeit des Widerspruchs Kenntnis erlangt, muss der Internet-Unternehmer diesen vorab informieren.

Und noch einen weiteren Wermutstropfen enthält die Regelung: In keinem Fall dürfen die pseudonymisierten Daten mit Klardaten, aus denen die Identität hervorgeht, zusammengeführt werden. Andernfalls würde es sich – was ja logisch ist – nicht mehr um pseudonymisierte Daten handeln.

Für die derzeitig vorherrschenden Formen der personalisierten Werbung reichen solche pseudonymisierten Benutzerprofile in der Regel aus, denn dem Werbetreibenden sind die Namen i. d. R. egal, viel wichtiger ist die genaue Zielgruppen-Ansprache.

b. Die Voraussetzungen im Einzelnen:

aa. Vorliegen eines Speicherungsgrunds

Die Speicherung pseudonymisierter Benutzerprofile ist für Zwecke der Werbung, der Marktforschung und der bedarfsgerechten Webseiten-Gestaltung erlaubt (§ 15 Abs. 2 S. 1 TMG).

Die Abgrenzung zwischen Marktforschung und Werbung ist in der Praxis nicht immer leicht und häufig sehr fließend. Eine anschauliche und leicht nachvollziehbare Abgrenzung bietet folgender Gedankengang: Marktforschung und Werbung betreffen beide den iden-

Anonyme Daten	Pseudonymisierte Daten	Klarden
= können keiner konkreten Person mehr zugeordnet werden, liegen nur noch vor	= Identifikationsmerkmale werden durch ein Pseudonym ersetzt	= vollständige Speicherung aller Daten
Rechtlich uneingeschränkt verwendbar	Es müssen drei Voraussetzungen vorliegen: 1. Speicherungsgrund 2. Kein Widerspruch 3. Keine Verbindung mit Klarden	Ohne Einwilligung nicht verwendbar für Online-Nutzungsprofile

tischen Gegenstand. Der entscheidende Unterschied ist lediglich die Betrachtungsweise. Die Marktforschung beschäftigt sich mit der Gewinnung neuer Erkenntnisse, die Werbung hingegen mit der Verwendung dieser neuen Erkenntnisse. Letzten Endes bedarf es hier jedoch keiner näheren Entscheidung, denn die Norm zählt beide Dinge als gleichberechtigte Möglichkeiten nebeneinander auf.

Der Speicherungsgrund „bedarfsge-rechte Gestaltung“ ist hingegen für die Werbevermarktung von Online-Nutzerprofilen weniger interessant, da er grundsätzlich nicht zur Speicherung von werberelevantem Handeln berechtigt.

bb. Kein Widerspruch

Der Nutzer darf der Erstellung des pseudonymisierten Benutzerprofils nicht widersprochen haben. Eine wichtige Bedeutung erlangt in diesem Zusammenhang die Aufklärungspflicht des Portal-Betreibers. Dieser muss nämlich den User zuvor über den Umstand der Pseudonymisierung und die Möglichkeit des Widerspruchs informieren.

Bei Internet-Portalen, die Nutzerprofile lediglich von registrierten Nutzern erheben, ist dies unproblematisch möglich. Im Rahmen der Anmeldung wird einfach auf diese Umstände hingewiesen, mehr ist nicht erforderlich.

Problematisch hingegen sind die Fälle, in denen Unternehmen auch Daten von nicht registrierten Usern

speichern, z. B. von allen Personen, die eine Webseite ansurfen. Hier stellt sich die entscheidende Frage, an welcher Stelle die rechtliche Aufklärung zu platzieren ist: direkt auf der Startseite mittels eines großen, bunt blinkenden Pop-up-Fensters? Oder reicht auch die dezente Platzierung im Impressum aus? Und genügt es, den Widerspruch in Form eines Opt-out-Cookies auf dem lokalen Rechner des Users zu speichern?

Überraschenderweise existiert zu diesem gesamten Themenkomplex bislang keinerlei Rechtsprechung in Deutschland. So unbefriedigend diese Tatsache auf den ersten Blick ist, sollten Sie als Internet-Unternehmer diesem Umstand vielmehr eine positive Seite abgewinnen: Wenn nämlich alles ungeklärt ist, so kann es Ihnen niemand vorwerfen, wenn Sie diesen Freiraum nutzen.

cc. Keine Zusammenführung mit Klarden

Das Gesetz verbietet es, die pseudonymisierten Daten mit Klarden, aus denen die Identität hervorgeht, zusammenzuführen.

Beispiel: Facebook speichert einmal Bestandsdaten in Form von Klarden. Also z. B. Vor- und Nachname, Straße, PLZ, Ort und Beruf („Martin Bahr, Mittelweg 41a, 20148 Hamburg, Rechtsanwalt“). Facebook legt nun einen

eigenen Datensatz für seine Nutzungsdaten an. Es entfernt alle identifizierbaren Informationen und ersetzt den Namen durch das Pseudonym „00001“. Übrig bleibt somit nur noch „00001, Hamburg, Rechtsanwalt“. Dieser neue Datensatz muss getrennt von o. g. Bestandsdaten gespeichert werden und darf auch zu keinem späteren Zeitpunkt mehr den Bestandsdaten zuzuordnen sein.

3. Klarden:

Ohne Einwilligung des Betroffenen ist die Erstellung von Online-Benutzerprofilen mit Klarden praktisch nicht durchführbar. Das Gesetz erlaubt zwar an einigen Stellen die Speicherung von Klarden (z. B. zu Abrechnungszwecken), jedoch nie zu Zwecken der Werbung oder Marktforschung.

Dabei soll die Einwilligung die eierlegende Wollmilchsau sein. Sie soll nicht nur die Speicherung der Daten für die unterschiedlichsten Zwecke erlauben, sondern auch die Verarbeitung und Zusammenführung von Daten und deren Weitergabe an Dritte. Es liegt auf der Hand, dass die Rechtsprechung für solche Zustimmungshandlungen kaum erfüllbare Voraussetzungen aufstellt. In der Praxis ist kaum eine der derzeitigen Einwilligungserklärungen rechtskonform². ¶

² RA Dr. Bahr „Rechtskonformes Opt-in im Online-Bereich“ (S. 950-957), in: „Leitfaden Online-Marketing: Band 2“, T. Schwarz (Hrsg.), 2011.