Ausgebremst

Rechtliche Schranken für Big-Data-Auswertungen

Unternehmen und Behörden übersehen bisweilen, dass sowohl das deutsche als auch das europäische Datenschutzrecht allzu ambitionierten Big-Data-Projekten Grenzen setzt. Allerdings bleiben graue Bereiche, die Unternehmen nur zu gerne ausnutzen.

Von Joerg Heidrich

Big Data lebt vom Sammeln und Kombinieren möglichst vieler Daten aus möglichst vielen Quellen. Oft ist es das Ziel, Menschen zu durchleuchten, zu bewerten und ihr Verhalten vorherzusagen. Doch genau solche „gläsernen Menschen" zu verhindern ist fundamentale Aufgabe und zentraler Inhalt des Datenschutzrechts.

Dies gilt zumindest dann, wenn es sich bei den verwendeten Informationen um personenbezogene Daten handelt. Das Bundesdatenschutzgesetz (BDSG) versteht darunter „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person".

Bei Informationen, die sich nicht auf einzelne Personen zurückführen lassen, greift der Datenschutz nicht. Dies gilt beispielsweise für ein Projekt über Verkehrsfluss, bei dem Informationen über Staus und die Gesamtanzahl der Verkehrsteilnehmer gesammelt und verarbeitet werden. Anders sähe es aus, würden für das Projekt gezielt das Verhalten einzelner Verkehrsteilnehmer erfasst und ausgewertet oder beispielsweise Kfz-Kennzeichen genutzt werden. Dann müsste eine Anonymisierung der Daten einer Auswertung vorausgehen.

Denn alle Daten, die eine Person bestimmbar machen, fallen unter den vom BDSG gewährten Schutz. Dies sind Informationen wie Name, Adresse, Geburtsdatum, aber auch genetische Daten, Telefonnummern oder die IP-Adresse des eigenen Rechners. Für derartige Angaben sieht das Gesetz ein sogenanntes „Verbot mit Erlaubnisvorbehalt" vor: Die Erhebung, Nutzung und Weitergabe sind grundsätzlich erst einmal verboten. Erst, wenn der Betroffene explizit eingewilligt hat oder ein Gesetz die Nutzung erlaubt, gilt das Verbot nicht mehr.

Diese Regeln gelten keineswegs nur für deutsche Unternehmen oder Behörden. Grundsätzlich müssen sich auch US-amerikanische Konzerne, die ihre Dienste deutschen Nutzern anbieten, an das BDSG halten. Derzeit tobt dazu an einigen Fronten ein erbitterter Streit. Facebook etwa verweist stets darauf, dass der europäische Firmensitz in Dublin ist und deshalb irisches Datenschutzrecht für den Konzern gelte. Wie die Sache ausgeht, ist noch unklar.

Informierte Einwilligung

Laut BDSG ist es auf jeden Fall erlaubt, auch intimste persönliche Informationen zu verwerten, wenn deren Träger sich damit einverstanden erklärt. Dies darf dem Betroffenen aber nicht in irgendeiner Form untergeschoben und zum Beispiel im Kleingedruckten der Nutzungsbedingungen versteckt werden. Vielmehr fordert das Gesetz eine explizite und „informierte Einwilligung", online in der Regel durch ein aktives Bestätigen eines Informationstexts. Und genau daran scheitert

häufig die freiwillige Erhebung von Daten für Big-Data-Projekte.

Nach Ansicht einiger Gerichte reicht beispielsweise die gängige Passage nicht aus, Daten „für Marketingzwecke" erheben zu wollen. Wer etwa Adressen erhebt, um „Newsletter über neue Zeitschriften und Veranstaltungen" zu versenden, muss dies auch genau so konkret benennen.

Was für derlei Zwecke noch praktikabel scheint, wird bei Big-Data-Sammelei fast unmöglich: Wollte man den Nutzern alle Anwendungsfälle und Auswertungsziele verständlich und detailliert erklären, würde ein Mammut-Text entstehen, den kaum ein User auch nur freiwillig lesen, geschweige denn abnicken würde.

Schwammige Gesetze

Da es deshalb mit einer wirksamen Einwilligung meist schwierig ist, bleibt für eine rechtlich wirksame Erhebung und Verwendung personenbezogener Daten nur eine andere gesetzliche Vorgabe. Dies führt zu den Generalklauseln der Paragrafen 28 und 29 BDSG, die allerdings alles andere als eindeutig daherkommen.

Wichtigste Generalklausel ist der Absatz 2 von Paragraf 28 BDSG. Danach ist es zulässig, geschützte Informationen für die Erfüllung eigener geschäftlicher Zwecke zu nutzen, wenn „es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt".

Die „Wahrung berechtigter Interessen" heißt im Klartext: Das Erheben und Verarbeiten der Daten muss von hoher Wichtigkeit für Geschäftszwecke des Unternehmens sein. Dazu gehören beispielsweise Maßnahmen zur IT-Sicherheit oder zur Fraud-Detection – etwa, um Betrugs- oder Korruptionsfälle aufzuspüren. Alles, was im weitesten Sinne in den Bereich des „Nice to have" fällt, genügt dagegen nicht. Hierunter fallen vor allem die meisten Marketing-Maßnahmen.

Außerdem ist immer eine Abwägung mit den Interessen des Betroffenen erforderlich. Als Ergebnis könnte es etwa zulässig sein, Kundeninformationen in einem CRM um zusätzliche Angaben zu erweitern. Die Grenze überschreitet das Unternehmen aber, wenn es Kundenprofile anlegt, um zielgerichtete Werbung zu ermöglichen.

Außer den Generalklauseln enthält das BDSG noch einige andere Möglichkeiten, Daten legal zu nutzen. So dürfen Unternehmen auch „allgemein zugängliche Daten" für eigene Geschäftszwecke verarbeiten, sofern nicht schutzwürdige Interessen des Betroffenen offensichtlich überwiegen.

Umstritten ist, ob dies auch für Plattformen gilt, die eine vorherige Anmeldung oder Authentifizierung erfordern. Die Mehrheit der Juristen und Datenschützer lehnt es ab, diese Vorschrift für zugangsbeschränkte Angebote wie Facebook anzuwenden. Der Datenerhebung in offenen Social-Media-Kanälen wie Twitter oder Google+ steht aber in aller Regel nichts im Weg.

Die Zweckbindung für gesammelte Daten ist ein „Big-Data-Killer".

Besonders strenge Regeln gelten für die Erfassung von sensiblen persönlichen Daten. Sogenannte „besondere Arten personenbezogener Daten" sind Angaben über die „rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben". Für solche Informationen gilt ein zusätzlicher Schutz, sodass es ohne Einverständnis rechtlich kaum möglich ist, sie etwa für Big-Data-Analysen zu nutzen. Vor allem im medizinischen Bereich führt diese Einschränkung zu aufwendigen Verfahren zur Anonymisierung von Patientendaten.

Zweckgebunden und sparsam

Selbst wenn das BDSG in manchen Fällen die Erhebung und Nutzung gestattet, sind es vor allem zwei allgemeine Grundsätze des Datenschutzes, die sich in der Praxis als größter Gegner von Big-Data-Analysen erweisen: die Datensparsamkeit und die Zweckbindung.

Erstere ist in Paragraf 3a BDSG verankert und gebietet, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Eine private „Vorratsdatenspeicherung" für nicht genau festgelegte Zwecke untersagt das Gesetz damit eindeutig. Genau diese ist aber de facto Grundlage zur massenhaften Verarbeitung möglichst großer Mengen von Daten, die benötigt werden, um aussagekräftige neue und belastbare Aussagen zu erhalten.

Einen regelrechten „Big-Data-Killer" stellt das von Unternehmen oft wenig geschätzte Prinzip der Zweckbindung dar. Danach dürfen sie personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erheben. Loggt ein Admin beispielsweise Website-Zugriffe der Besucher, um die IT-Sicherheit zu gewährleisten, dürfen diese Daten eben nicht zu Marketing-Zwecken genutzt werden. Dieser Grundsatz schließt in der Praxis sehr viele Fälle von Datenzusammenführung und -analyse aus. Eine Verarbeitung zu anderen Zwecken als den ursprünglich bei der Erhebung vorgesehenen, also quasi eine Umwidmung, ist nur sehr eingeschränkt in Einzelfällen legal.

Der Königsweg für Big-Data-Projekte liegt daher hierzulande darin, so weit wie möglich auf personenbezogene Daten zu verzichten oder diese zu anonymisieren, beziehungsweise wenigstens zu pseudonymisieren.

Wesentliche Änderungen dieser recht komplizierten Rechtslage dürfte auch der neue europäische Datenschutz nicht bringen. Insbesondere enthält die 2018 in Kraft tretende Datenschutzgrundverordnung (DSGVO), die dann die bisherigen deutschen Regelungen komplett ersetzt, auch die Grundsätze der Zweckbindung und der Datensparsamkeit. An einer speziellen Regelung für Big-Data-Projekte fehlt es, was zu heftiger Kritik von Unternehmen führte.

Was sich allerdings ändert, sind die Sanktionsmöglichkeiten in Form von Geldstrafen durch die zuständigen Aufsichtsbehörden. Während das BDSG maximal 300.000 Euro für gravierende Verstöße vorsieht, werden mit der DSGVO Bußgelder bis zu 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes möglich. Dies dürfte die Motivation von europäischen, aber auch US-amerikanischen Unternehmen steigern, sich auch im Detail an den europäischen Datenschutz zu halten.

(hob@ct.de) ct