ZEITSCHRIFT FÜR DATENSCHUTZ

ZD

EDITORIAL

3/2011

„Personenbezogene Daten“ aus internationaler Perspektive

Das Datenschutzrecht beruht in erster Linie auf dem Konzept der „personenbezogenen Daten.“ Informationen innerhalb dieser Kategorie sind geschützt, Informationen außerhalb sind es nicht. Angesichts der zentralen Bedeutung des Konzepts der personenbezogenen Daten erscheint es überraschend, dass es keine weltweit übereinstimmende Definition dieses Begriffs gibt.

Der Mangel an Einheitlichkeit hinsichtlich eines so grundsätzlichen Konzepts hat erhebliche Auswirkung im Zeitalter der globalen Datenübertragung. Informationen, die in Deutschland als personenbezogene Daten angesehen werden, unterfallen möglicherweise keinerlei Datenschutzbestimmungen in den Vereinigten Staaten.

Darüber hinaus führt die weltweite Entwicklung der Informationstechnologie zu einer Verschiebung der Grenze zwischen personenbezogenen und sonstigen Daten. In vielen Fällen ist es daher schwierig bereits im Vorfeld zu entscheiden, ob bestimmte Informationen personenbezogene Daten sind oder nicht. Aus diesen Gründen sollte den unterschiedlichen nationalen Definitionen des Begriffs der personenbezogenen Daten sowie dem Erfordernis der Bemühungen um eine globale Harmonisierung in Zukunft größere Bedeutung beigemessen werden.

Prof. Paul M. Schwartz
lehrt an der Berkeley Law School, ist Direktor des Berkeley Center for Law & Technology und Mitglied des Wissenschaftsbeirats der ZD.

„Personenbezogene Daten“ im Recht der Europäischen Union und nach deutschem Recht

Sowohl das Recht der Europäischen Union als auch das deutsche Recht folgen bei der Definition des Konzepts der persönlichen Daten einem extensiven Ansatz. Demzufolge definiert die EU-Datenschutzrichtlinie „personenbezogene Daten“ als „Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person‘)“, wobei eine Person als bestimmbar angesehen wird, „die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“ (Art. 2 lit. a 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, ABl. L 281 v. 23.11.1995, S. 31–50).

Als Auslegungshilfe nennt die Richtlinie in Erwägungsgrund Nr. 26 außerdem, dass „(b)ei der Entscheidung, ob eine Person bestimmbar ist, … alle Mittel berücksichtigt werden (sollten), die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen“ (a.a.O., Erwägungsgrund 26).

Mithin werden nach EU-Recht Informationen über eine „bestimmbare“ Person genauso behandelt wie Informationen, die sich auf eine „bestimmte“ Person beziehen. Dieses Konzept der Gleichstellung von „bestimmten“ und „bestimmbaren“ Personen ist als deutsche Innovation im Bereich des Datenschutzrechts anzusehen. Die Berücksichtigung potenzieller Gefahren ausgehend von Daten über „bestimmbare“ Personen fand bereits in der ersten Fassung des Bundesdatenschutzgesetz (BDSG) von 1977 Ausdruck. Zu dieser Zeit bestand die Befürchtung, dass die zunehmende Verwendung von Computern in Kombination mit den neuen Möglichkeiten des Datenverarbeitungsmanagements zu einer Re-Individualisierung von Daten führen könnte.

Entsprechend definiert das BDSG auch heute „personenbezogene Daten“ sowohl als Informationen über „bestimmte“ als auch über „bestimmbare“ Personen. Die entscheidende Regelung findet sich in § 3 Abs. 1 BDSG, in welchem „personenbezogene Daten“ als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“ definiert sind.

Die Gleichstellung von „bestimmten“ und „bestimmbaren“ Personen war vorausschauend und von großer Bedeutung für die Internationalisierung des Datenschutzes. Im Anschluss an die Auslegung im BDSG definieren beispielsweise die datenschutzrichtlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD-Richtlinien) „personenbezogene Daten“ als „alle Informationen, die sich auf eine bestimmte oder bestimmbare Person (Datensubjekt) beziehen.“
Ebenso wie die OECD-Richtlinien legt auch das Privacy Framework der Asiatisch-Pazifischen Wirtschaftlichen Zusammenarbeit (APEC-Framework) personenbezogene Daten als „alle Informationen, die sich auf eine bestimmte oder bestimmbare Person“ beziehen, aus.

„Personenbezogene Daten" im Recht der Vereinigten Staaten

Wie werden nun in den Vereinigten Staaten „personenbezogene Daten" (Personally Identifiable Data bzw. PII) definiert? Zusammen mit *Daniel Solove* habe ich (*Paul M. Schwartz/Daniel J. Solove*, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 2011, i.E.) eine Typologie der unterschiedlichen Definitionen im US-amerikanischen Recht vorgenommen und drei Definitionsmodelle identifiziert (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366).

- Das erste Modell ist tautologisch. Personenbezogene Daten werden dort als jegliche Information angesehen, durch die eine Person identifiziert werden kann. Der Video Privacy Protection Act folgt z.B. einem solchen Modell. Danach sind „personenbezogene Daten" definiert als „Informationen, die eine Person identifizieren"(Video Privacy Protection Act, 18 U.S.C. § 2710 (a) (3)).
- Das zweite Modell deutet personenbezogene Daten als nicht-öffentliche Daten. Anstatt einer direkten Begriffsbestimmung der personenbezogenen Daten wird der Begriff jedoch indirekt durch den Bereich, der keine personenbezogenen Daten umfasst, festgelegt. Der nicht-öffentliche Ansatz besagt konkret, dass personenbezogene Daten nicht-aggregierte Daten sind. Geradezu ein Inbegriff dieses Ansatzes findet sich im Gramm-Leach-Bliley Act, der „personenbezogene Daten" als „nicht-öffentliche persönliche Informationen" definiert (Gramm-Leach-Bliley Act, 15 U.S.C. § 6809 (4) (A); s.a. *Daniel J. Solove/Paul M. Schwartz*, Privacy Law Fundamentals, 4. Aufl. 2011, S. 91–92).
- Schließlich existiert ein drittes Modell, wonach bestimmte einzelne Kategorien von Daten aufgezählt werden, die personenbezogene Daten darstellen. Nach diesem Modell sind Daten per se personenbezogen, sofern sie in eine gesetzlich aufgezählte Kategorie fallen. Der Children's Online Privacy Protection Act of 1998 macht von diesem Modell Gebrauch. Er zählt die persönlich relevanten Daten auf, wozu u.a. Vor- und Nachname sowie ferner Postadresse, Sozialversicherungsnummer, Telefonnummer und E-Mail-Adresse gehören (Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (8) (A) – (E)).

Wir sind der Meinung, dass alle drei US-amerikanischen Modelle nicht fehlerfrei sind. Der tautologische Ansatz basiert erkennbar auf einem Zirkelschluss. Der nicht-öffentliche Ansatz versucht zu definieren, welche Daten nicht personenbezogen sind, wobei jedoch die angewandte Unterscheidung zwischen öffentlicher und privater Natur von Daten nicht die Frage nach der Bestimmbarkeit einer Person zu lösen vermag. Schließlich kann auch das Modell der Einzelfallaufzählung keine Definition anbieten – es listet nur spezifische Fälle auf, stellt jedoch keinerlei Konzepte oder Methoden zur Verfügung, um die Art der Informationen zu kategorisieren, die in der Liste enthalten sind oder nicht.

Probleme und Lösungen

Aus US-amerikanischer Sicht besteht die mögliche Gefahr des deutschen Ansatzes darin, dass ein zu großer Bereich von Daten als „bestimmbar" angesehen wird – selbst wenn die Möglichkeit der Identifizierung verhältnismäßig gering ist. Umgekehrt könnten die US-amerikanischen Ansätze aus deutscher Sicht als verwirrend und uneinheitlich empfunden werden. Aus US-amerikanischer Binnensicht besteht substanziell die Gefahr der Manipulation der Datensammlung und -verarbeitung durch Unternehmen und andere dem Datenschutz unterworfene Stellen zum Zweck der Vermeidung der Datenschutzbestimmungen. Beispielsweise identifizieren Unternehmen beim Behavioral Marketing Individuen nicht anhand ihres Namens. Stattdessen setzen sie Software zur Erstellung von Persönlichkeitsprofilen ein, die den Namen nicht beinhalten, jedoch eine Vielzahl von Detailinformationen über das Individuum enthalten. Diese Persönlichkeitsprofile sind verbunden mit einem einzelnen alphanumerischen Code, der im Computer des Individuums gespeichert ist. Unternehmen sind oft der Auffassung, dass diese Daten keine personenbezogenen Daten darstellen und daher nur ein reduziertes Datenschutzbedürfnis daran bestünde.

Vor diesem Hintergrund und der dafür maßgeblichen Bedeutung des Begriffs der „personenbezogenen Daten" haben *Daniel Solove* und ich für das US-amerikanische Recht das Konzept „Personally Identifiable Information 2.0" (PII 2.0) entwickelt. Wir sind der Meinung, dass rechtliche Datenschutz- und Sicherheitsstandards sowohl für bestimmte als auch bestimmbare Personen vorhanden sein müssen. Die Standards müssen ferner an die vorherrschenden Risikolevels angepasst werden. Im Allgemeinen stellen Daten, die eine Person lediglich bestimmbar machen, jedoch noch nicht endgültig bestimmen, ein vermindertes Datenschutzrisiko dar. Ferner schlagen wir vor, dass Daten über bestimmbare Personen als Daten über bestimmte Personen angesehen werden, sobald eine erhebliche Wahrscheinlichkeit existiert, dass die Daten verlinkt und einer bestimmten Person zugeordnet werden.

Die gerade dargestellte Art der Risikoberücksichtigung ist auch dem deutschen Datenschutzrecht nicht fremd. So hat beispielsweise *Ulrich Dammann* den Bestimmbarkeitsgrundsatz als relativen Standard diskutiert: „Praktisch ausgeschlossen ist die Bestimmbarkeit, wenn die Wahrscheinlichkeit einer erfolgreichen Bestimmung so gering ist, dass das Risiko praktisch vernachlässigt werden kann" (*Damann*, in: Simitis (Hrsg.), BDSG., 7. Aufl. 2011, § 3 Rdnr. 23). In diesem Zusammenhang weist *Dammann* auch auf die Bedeutung des Informationswerts hin, d.h. „der Personenbezug ist ... zu verneinen – wenn der Aufwand den Informationswert so wesentlich übertrifft, dass man vernünftigerweise davon ausgehen kann, dass niemand den Versuch der Personenbestimmung unter Verwendung der betreffenden Daten unternehmen wird" (a.a.O., Rdnr. 25; s.a. *Art. 29-Datenschutzgruppe*, WP 136, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", III.3).

Allgemein bleibt festzustellen, dass die Rechtssysteme in verschiedenen Ländern – im Fall der Vereinigten Staaten sogar in demselben Land – derzeit unterschiedliche Ansätze zur Definition „personenbezogener Daten" haben. Es ist zu hoffen, dass das PII 2.0-Konzept zu einer gewissen Vereinheitlichung und Weiterentwicklung des Datenschutzrechts in den Vereinigten Staaten und eine Annäherung an bekannte europäische Konzepte beitragen kann. Um jedoch ein wirklich globales Datenschutzrecht zu erreichen, müssen sich die Bemühungen langfristig auf die Frage nach der Harmonisierung sämtlicher verschiedener nationaler und internationaler Konzepte konzentrieren. Dies ist sicherlich eine der wichtigsten Aufgaben für die Zukunft des Datenschutzrechts in den kommenden Jahren und Jahrzehnten.