ZEITSCHRIFT FÜR DATENSCHUTZ

ZD

EDITORIAL

3/2020

Sind manche Datensätze schützenswerter als andere?

Lesedauer: 9 Minuten

Das neue Jahrzehnt hat für den Datenschutz mit Fanfarenstößen begonnen. Besonders sticht eine neue Entscheidung des *Europäischen Gerichtshofs für Menschenrechte* (*EGMR*) in Straßburg heraus. Der *EGMR* hat am 30.1.2020 – App. No. 50001/12 (Rs. Breyer vs. Germany) nach Jahren des Prozessierens den im TKG festgelegten Identifizierungszwang für Mobilfunkkarten bestätigt. Die Speicherpflicht im TKG für Prepaid-Verträge verstoße nicht gegen das Prinzip der Verhältnismäßigkeit. Diese Frage an der Nahtstelle zwischen TK-Recht, Strafverfolgungsinteresse und Datenschutzrecht beschäftigt die Öffentlichkeit schon seit Jahren.

Interessant in diesem Zusammenhang ist zunächst folgende Passage (Rdnr. 90): „Der Gerichtshof weist erneut darauf hin, dass die nationalen Behörden im Zusammenhang mit der nationalen Sicherheit einen gewissen Ermessensspielraum bei der Wahl der Mittel zur Erreichung eines legitimen Ziels haben, und stellt fest, dass nach dem rechtsvergleichenden Bericht kein Konsens zwischen den Mitgliedstaaten hinsichtlich der Speicherung von Teilnehmerdaten von Prepaid-Sim-Karten-Kunden besteht."

Dr. Axel Spies
ist Rechtsanwalt bei Morgan, Lewis & Bockius LLP in Washington DC und Mitherausgeber der ZD.

Mit anderen Worten: Der fehlende Konsens in Europa wirkt sich hier zu Lasten des Antragstellers aus. Dies dürfte die Konsensfindung der verantwortlichen Behörden und Parlamente in der EU nicht gerade erleichtern.

Zweitens, und wohl im Grundsatz wichtiger, streicht der *EGMR* im Einklang mit dem *EuGH* in der Rs. Ministerio Fiscal (C-207/16, hier: gestohlene SIM-Karten) heraus, dass die abgespeicherten Daten es nicht ermöglichen, „Datum, Uhrzeit, Dauer und Empfänger der mit der oder den fraglichen SIM-Karte(n) durchgeführten Kommunikationen zu ermitteln, ebenso wenig wie die Orte, an denen diese Kommunikationen stattfanden, oder die Häufigkeit dieser Kommunikationen mit bestimmten Personen während eines bestimmten Zeitraums. Diese Daten lassen daher keine genauen Rückschlüsse auf das Privatleben der Personen zu, deren Daten betroffen sind" (Rdnr. 94).

Beide *Gerichte* greifen damit den Faden auf, den das *BVerfG* mit dem Schutz des „absolut geschützten Kernbereichs privater Lebensgestaltung" nach Art. 10 GG gesponnen hat (u.a. U. v. 3.3.2004 – 1 BvR 2378/98, MMR 2004, 302). Daten innerhalb dieses Kernbereichs gelten als besonders schützenswert. Diese Abstufung für hochpersönliche Daten ist ein interessanter Ansatz, weil das *BVerfG* seit dem Volkszählungsurteil von 1983 wie auch Art. 4 Nr. 1 DS-GVO beim Datenschutz eigentlich vom ehernen Grundsatz ausgehen, dass es „kein unbedeutendes Datum gibt."

Dahinter steht die im Volkszählungsurteil näher ausgeführte Befürchtung, dass der Bürger zum „gläsernen Menschen" werde, wenn an sich unbedeutende Datensätze mit anderen Datensätzen kombiniert werden. „Selbst die Information, dass Person X zwei Arme hat, stellt ein personenbezogenes Datum dar" (*Klar/Kühling,* in: Kühling/Buchner, DS-GVO, Art. 4 Nr. 1 Rdnr. 9).

Gesetzlich angelegte Abstufungen

Trotz dieses Prinzips kommt man um Abstufungen, je nachdem wie wichtig das Datum für die betroffene Person ist („hochpersönlich") oder ob besondere Risiken bestehen, im Datenschutz nicht herum. Im Prinzip ist so eine Unterscheidung schon in Art. 9 Abs. 1 DS-GVO angelegt, weil der Gesetzgeber dort folgende personenbezogene Daten pauschal als besonders schützenswert eingestuft hat: die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit, die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Ob es in diesen Bereichen mögliche Abstufungen nach oben oder unten gibt, ist offen. Andere Beispiele für besonders gesetzlich geregelte Datensätze sind: der Wahrscheinlichkeitswert bei Scoring und Bonitätsauskünften (§ 31 BDSG), die deutsche Steuer-ID (§ 139b AO), Krankenversicherungsnummer (§ 290 f. SBG V), Reisepassnummer (§ 16 PassG) oder allgemein die Regelung über die nationale Kennziffer in Art. 87 DS-GVO.

Praxis in den USA

Eine Abstufung, nach der manche personenbezogenen Datensätze besonders schützenswert sind (oder zumindest anders zu behandeln sind), ist in den USA gängige Praxis.

■ Der neue, seit dem 1.1.2020 geltende California Consumer Privacy Act (CCPA) ist mit seinen elf Kategorien von „personal information" breit angelegt, bleibt aber hinter der pauschalen Regelung in Art. 4 Nr. 1 DS-GVO zurück, da der Verbraucherschutz im Vordergrund steht.

- Das neue Konsumenten-Datenschutzgesetz von Nevada deckt nur sieben Datenkategorien ab, nämlich: (1) Vor- und Nachnamen; (2) Wohnadresse oder eine andere physische Adresse; (3) E-Mail-Adresse; (4) Telefonnummer; (5) Sozialversicherungsnummer; (6) eine Kennung, die es ermöglicht, eine bestimmte Person entweder physisch oder online zu kontaktieren; (7) alle anderen Informationen über eine Person, die von der Person über die Website oder den Onlinedienst des Betreibers gesammelt wurden.

- Das neue Online Privacy Law des Staats Maine schützt: Webbrowser-Verlauf, Geolokalisierungsdaten, Gerätekennungen, die Ursprungs- und Ziel-IP-Adressen, persönliche Identifizierungsdaten und den Inhalt der Kommunikation des Nutzers in Maine.

- Anders wiederum die Lage im Staat New York. Dort tritt am 21.3.2020 ein weiteres Maßnahmen-Paket des SHIELD Act in Kraft. Alle Unternehmen weltweit, die bestimmte Daten von Einwohnern des Staats New York sammeln, müssen spätestens ab dann angemessene Sicherheitsvorkehrungen in der Hinterhand haben, welche die Sicherheit, Vertraulichkeit und Integrität der vom SHIELD Act abgedeckten privaten Informationen schützen. Dazu zählen etwa die Benennung von Cybersicherheitspersonal, die Durchführung angemessener Kontrollen zum Schutz personenbezogener Daten, die Durchführung von Mitarbeiterschulungen etc. Auch hier sind nicht alle personenbezogenen Daten abgedeckt, sondern (nur) die Sozialversicherungs-, Führerschein- oder Personalausweis-, Konto-, Kredit- oder Debitkarten-Nummer sowie biometrische Informationen. Biometrische Informationen sind hier genauer definiert als Daten, die durch elektronische Messungen der individuellen physischen Merkmale einer Person erzeugt werden, wie eine Fingerabdruck- und Stimmenanalyse oder ein Netzhaut- bzw. Iris-Scan.

- Das wegweisende Gesetz von Massachusetts zum Schutz der Personen bei einem Bruch der Datensicherheit und damit einhergehenden strengen Meldepflichten umfasst gegenwärtig abschließend folgende Kategorien: Vorname und Nachname des Einwohners oder Initiale des Vornamens plus Nachname, aber nur in Kombination mit einem oder mehreren der folgenden Datenelemente: Sozialversicherungsnummer, Nummer des Führerscheins oder des staatlich ausgestellten Personalausweises oder Kontonummer der Person oder der Kreditkarte, mit oder ohne erforderlichen Sicherheits-/Zugangscode.

- Hingegen schützt das sehr detaillierte, mehrfach geänderte Bundesgesetz Health Insurance Portability And Accountability Act (HIPPA) von 1996 zahlreiche genau definierte Datensätze der Patienten im Gesundheitsbereich. Bestimmte Finanzdaten schützt der Gramm-Leach-Bliley Act von 1999 mit Sonderregeln.

Eingrenzung der Meldeflut

Angesichts der rapide wachsenden Datenflut weltweit werden Spezialgesetze oder -regelungen für bestimmte Datenkategorien in Zukunft im Datenschutz stärker eine Rolle spielen müssen. Ein Bedürfnis nach eine Abstufung besteht überall, da mehr und mehr Daten maschinell erfasst werden, deren Verarbeitung von der Datenschutzaufsicht kaum noch nachgehalten werden kann. Für manche Datenkategorien gibt es technische Besonderheiten (z.B. für die Verkehrs- und Standortdaten in der ePrivacy-RL), die angemessen zu berücksichtigen sind.

Eine Abstufung spielt schon gegenwärtig bei der Auslegung bestehender DS-GVO-Vorschriften eine Rolle, z.B. bei der Abwägung der berechtigten Interessen in Art. 6 Abs. 1 lit. f DS-GVO, wo die Kommentatoren auf die „Aussagekraft der Daten" und die „vernünftigen Erwartungen der betroffenen Person" abstellen (u.a. *Buchner/Petri*, in: Kühling/Buchner, a.a.O., Art. 6 DS-GVO, Rdnr. 151 f.). Aber es bedarf bei der Abstufung des rechten Maßes, denn sonst kommt es dazu, dass sich in der EU unterschiedliche Auffassungen zu den Datenkategorien bilden.

Eine Einschränkung auf bestimmte Datensätze macht z.B. bei den Meldungen bei einem Bruch der Datensicherheit (Art. 33 DS-GVO) Sinn, um die Aufsichtsbehörden aus der Lawine der Meldungen „freizuschaufeln." Im Tätigkeitsbericht des *BayLDA* für 2018 heißt es u.a.: „Die Zahl der Meldungen zu Datenschutzverletzungen explodierte förmlich durch die DS-GVO. Insgesamt 2.471 Meldungen gingen im Jahr 2018 ein – sage und schreibe 2.376 davon seit dem 25. Mai 2018. Dies ist ein absoluter Rekordwert in unserer Geschichte als bayerische Aufsichtsbehörde" (*BayLDA*, TB 2018, S. 18). Für 2019 liegen die Zahlen vermutlich noch höher. Diese Menge – nur für Bayern – verwundert nicht. Bei der britischen Aufsichtsbehörde *ICO* sind es derzeit mehr als 1.276 Meldungen von Datenschutzverstößen pro Monat!

Die Leitlinien der *Art. 29-Datenschutzgruppe* (WP 250rev.1) v. 2.2.2018 für die Meldung von Verletzungen des Schutzes personenbezogener Daten enthalten trotz ihres Umfangs von 40 Seiten jede Menge Unsicherheiten, z.B. wenn ein bedauernswerter Mitarbeiter aus Versehen eine E-Mail an falsche Empfänger schickt. Was bedeutet die Maßgabe der *Art. 29-Datenschutzgruppe*, dass „die Benachrichtigung ... unter Umständen (!) nicht erforderlich [ist], wenn keine sensiblen Daten offengelegt werden und nur eine kleine Anzahl von E-Mail-Adressen sichtbar ist" (S. 39)?

Die Praxis lehrt uns: Die Verantwortlichen melden im Zweifel jeden Vorfall, wozu sie auch von ihrer Versicherung angehalten werden – nach der Devise „better safe than sorry". Die Aufsichtsbehörden sollten sich aber auf die wichtigen Fälle konzentrieren können. Insofern könnten die engeren Vorschriften zur Meldepflicht wie in Massachusetts durchaus ein Vorbild sein.