Bankgeschäfte und Einkaufen im Netz >
< Sehen und gesehen werden

Vorratsdatenspeicherung – ja oder nein?

Zwischen Ermittlungsgrundlage und Datenschutz

Die Vorratsdatenspeicherung könnte polizeiliche Ermittlungen vorantreiben

Die Speicherung von Verkehrsdaten, also der Aufzeichnung wesentlicher Verbindungsdaten wie etwa der IP-Adresse oder dem Standort einer Person, hat die Meinungen von Gesetzgebern, Polizei und Datenschützern in den letzten Jahren gespalten. Datenschützer fürchten um die Privatsphäre des Einzelnen. Denn dadurch würden sämtliche Telekommunikations- und Standortdaten ohne konkreten Anlass abgespeichert, wodurch jeder Mensch potenziell rund um die Uhr überwacht werden könnte. Die Polizei argumentiert, dass sie diese Daten hingegen dringend benötigt, um im Bereich Cybercrime effizient ermitteln zu können. Als Beispiel führt sie etwa den Fall eines 13-jährigen Mädchens an, das von einem unbekannten Mann über das Internet sexuell erpresst wurde. Hier erhielt die Polizei über den Betreiber der Internetplattform zwar aussagekräftige Log-Daten inklusive IP-Adressen, doch mangels einer Vorratsdatenspeicherung konnten diese Daten keiner konkreten Person zugeordnet werden.

Daten würden nur in konkreten Verdachtsfällen abgerufen werden

Im Jahr 2016 wurden 253.290 Straftaten erfasst, die mithilfe des Internets begangen wurden. Dazu gehören Betrugsdelikte und Computersabotage genauso wie die Verbreitung von Kinderpornografie. Bei vielen dieser Straftaten kann jedoch nicht ermittelt werden, weil die Internet-Verbindungsdaten bei den Telekommunikationsanbietern entweder gar nicht oder nur für eine sehr kurze Zeit gespeichert werden. Das Bundeskriminalamt hat ein umfangreiches Archiv angelegt, in dem zahlreiche Fälle dokumentiert sind, die mangels Vorratsdatenspeicherung unaufgeklärt blieben. „Die Bekämpfung der Internetkriminalität ist ohne eine Vorratsdatenspeicherung kaum denkbar. Es ist für die Polizei wichtig,

Zugang zu diesen Verbindungsdaten zu erhalten, da sie oft die einzige Spur sind, die zu den Tätern führt“, fordert Sascha Braun, Justiziar der Gewerkschaft der Polizei (GdP). Dabei ginge es nicht darum, der Polizei per se sämtliche Daten zur Verfügung zu stellen, sondern nur in konkreten Verdachtsfällen bei bestimmten Straftaten und nach richterlicher Anordnung. „Die Daten würden nicht von der Polizei gesammelt und gespeichert, sondern ausschließlich bei den Providern – und dort, wenn nötig, von der Polizei abgefragt. Diese Daten sind bereits größtenteils vorhanden, sie müssen nur für einen längeren Zeitraum zur Verfügung stehen“, erklärt er.

Schwierigkeiten bei der Gesetzgebung

Sascha Braun

Justiziar der GdP, © GdP

In Deutschland wurde im Jahr 2015 ein Gesetz zur Vorratsdatenspeicherung verabschiedet. Nach diesem Gesetz wurden alle Provider dazu verpflichtet, die Daten ihrer Nutzer ab dem 1. Juli 2017 für einen Zeitraum von zehn Wochen zu speichern. Diese anlasslose Speicherung von Daten wurde jedoch vom Europäischen Gerichtshof (EuGH) vor Inkrafttreten des Gesetzes aus Datenschutzgründen als illegal eingestuft. Durch einen Beschluss des Oberverwaltungsgerichts NRW, das eine Klage auf Grundlage der Entscheidung des EuGH vorliegen hatte, ist das Gesetz aktuell „faktisch ausgesetzt“. Das heißt, dass die Bundesnetzagentur keinen Provider zur Datenspeicherung zwingen kann. Bei einer endgültigen Entscheidung zu diesem Thema müssten die Gesetzgeber abwägen, wie lange eine entsprechende Speicherung der Daten für erfolgreiche polizeiliche Ermittlungen nötig wäre, und ob man den Umfang der abgespeicherten Daten nach bestimmten Kriterien eingrenzen könnte, damit nicht die Telekommunikationsdaten der gesamten Bevölkerung gesammelt werden. Es wird spannend bleiben, ob nationale und internationale Gesetzgeber in den nächsten Jahren eine Lösung finden werden, die sowohl den Bedenken der Datenschützer als auch den Forderungen der Polizei gerecht wird. Bis dahin dürfen die Provider selbst darüber entscheiden, ob sie die Daten ihrer Nutzer speichern oder nicht. Ein Großteil der Provider hat sich bislang dagegen ausgesprochen.
FL (29.09.2017)

Folgende Artikel könnten Sie auch interessieren:

- Das vernetzte Auto
- Urheberrecht im Internet
- Wer will an meine Daten?

Alle Artikel dieser Kategorie

Weitere Infos zum Thema Internet und Mobil

Zwischen Datenlecks, Bequemlichkeit und Onlinegeschäften

Die Kommunikationswelt der Zukunft

In den vergangenen Jahren kam es immer wieder zu Datenlecks, bei...[mehr erfahren]

Wie sicher sind funkfähige Kredit- und Girokarten?

Kontaktloses Bezahlen

Das Bezahlen an der Kasse soll mit funkfähigen Kredit- und EC-Karten...[mehr erfahren]

Projekt „Bottom-Up“ trägt Wissen in Unternehmen

IT-Sicherheit für Berufsschüler

Besonders kleine und mittelständische Unternehmen tun sich beim...[mehr erfahren]

Das Polizeipräsidium Stuttgart hat über 46.000 Facebook-Fans

Die Polizei auf Facebook und Twitter

Für die Polizeipräsidien sind Soziale Medien ein wichtiger Kanal, um...[mehr erfahren]

Eltern sollten Inhalte genau prüfen

Riskante Spiele-Apps

Spiele-Apps für das Smartphone wie „Angry Birds“, „Candy Crush“ oder...[mehr erfahren]