B undes
A rbeitskreis
C hristlich
D emokratischer
J uristen

CDU

Erforderlichkeit der Vorratsdatenspeicherung

- Fachkommission Strafrecht und Strafprozessrecht des BACDJ -

Der Staat hat eine aus den Grundrechten folgende Schutzpflicht, für die Sicherheit seiner Bürger zu sorgen. Eine effiziente Gestaltung der Sicherheitsarchitektur ist dafür unabdingbar. Ohne die erforderlichen Instrumente sind die Möglichkeiten der Ermittlungsbehörden jedoch eingeschränkt. Eines dieser Instrumente ist die Analyse von Kommunikationsdaten; sie ist in der modernen, digitalisierten Welt zur Aufklärung von Straftaten wichtiger denn je.

I. Bestandsaufnahme

Im Dezember 2015 ist in Deutschland das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BGBl. 2015 Teil I, S. 2218) in Kraft getreten. Es führt eine anlasslose, dauerhafte und flächendeckende Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten ein. Danach wurde den zur Speicherung verpflichteten Unternehmen auferlegt, diese Verpflichtung spätestens ab 1. Juli 2017 zu erfüllen (§ 150 Abs. 13 TKG).

Nach alter Rechtslage, vor Erlass des § 113b TKG, konnten die Strafverfolgungsbehörden die retrograden Verkehrsdaten, die von den Providern nach § 96 TKG etwa zu Abrechnungszwecken gespeichert werden, von diesen ermittlungsrichterlich angeordnet (§ 100g StPO) anfordern. Die Speicherdauer war zwischen den Providern uneinheitlich; ob und was gespeichert wurde, hing von den Vertragsbedingungen im Einzelfall ab. Mit der Einführung von § 113b TKG wurde zugleich § 12 EGStPO eingeführt, der für die Übergangsfrist von 1 ½ Jahren die Nutzung der Daten nach § 96 TKG weiter gestattet, endend zum 29. Juli 2017.

Mit Urteil vom 21. Dezember 2016 hat der Europäische Gerichtshof auf die Vorlage nationaler Regelungen der Mitgliedsstaaten Schweden und des Vereinigten Königreichs festgestellt, dass es europäischem Recht widerspreche, Vorratsdatenspeicherung flächendeckend, unterschieds- und anlasslos vorzuschreiben. Außerdem müsse, soweit dennoch gespeichert werde, der behördliche Zugang der vorherigen Kontrolle einer unabhängigen Instanz unterworfen werden.

Das Oberverwaltungsgericht Münster hat die in Deutschland geltende Rechtslage daraufhin für europarechtswidrig befunden. Es hat am 22. Juni 2017 entschieden, die ab dem 1. Juli 2017 zu beachtende Pflicht für die Erbringer öffentlich zugänglicher Telekommunikationsdienste, die bei der Nutzung von Telefon- und Internetdiensten anfallenden Verkehrs- und Standortdaten ihrer Nutzer für eine begrenzte Zeit von zehn beziehungsweise (im Fall von Standortdaten) vier Wochen auf Vorrat zu speichern, damit sie im Bedarfsfall den zuständigen Behörden etwa zur Strafverfolgung zur Verfügung gestellt werden können, sei mit dem Recht der Europäischen Union nicht vereinbar.

Die Bundesnetzagentur hat dieser Entscheidung die Folge gegeben, keinen Provider zu sanktionieren, der – contra legem – keine Daten liefert. Entsprechende Beschlüsse laufen seitdem, soweit sie überhaupt noch erlassen werden, regelmäßig ins Leere. Zudem besteht das Risiko eines Verwertungsverbotes.

Im Ergebnis stehen Verkehrsdaten für die Aufklärung von Straftaten nicht mehr zur Verfügung.

II. Erheblicher Nutzen der „Vorratsdatenspeicherung“

Verkehrsdaten sind bei der Polizeiarbeit in verschiedenen Konstellationen und unterschiedlicher Form von Bedeutung:

1. Zuordnung von IP-Adressen

Durch die Zuordnung von IP-Adressen zu einer Person kann etwa herausgefunden werden, wer Kinderpornografie auf einer Internetseite aufgerufen hat. Der Austausch von kinder- und jugendpornografischem Material, von entsprechenden Bildern und Videos, findet inzwischen weitgehend über das Internet statt. Beispielhaft wurden im Jahr 2014 über 6.000 Fälle des Besitzes und der Verbreitung von kinderpornografischem Material in der Polizeilichen Kriminalstatistik registriert. Ohne die Möglichkeit die genutzten IP-Adressen Personen zuzuordnen, können die Sicherheitsbehörden diese Täter nur schwer und häufig nicht identifizieren. Ebenso liegt es bei Betrugsstraftaten, die häufig im Internet begangen werden oder auch bei Cyberangriffen, die jeden Bürger treffen können, um seine Geräte für Botnetze zu missbrauchen.

2. Auswertung von Funkzellendaten

Mit Funkzellendaten kann im Einzelfall festgestellt werden, welches Mobiltelefon wann in welcher Funkzelle eingeloggt war bzw. wann ein Kommunikationsvorgang stattfand. Dies lässt, je nachdem wie groß die Funkzelle ist, Rückschlüsse zu, wo sich das Mobilfunkendgerät (bzw. die SIM-Karte) wann befand. So kann etwa aufgeklärt werden, wer sich an einem Tatort, an dem beispielsweise ein Mord geschehen ist, aufgehalten hat.

3. Auswertung von Telekommunikationsverkehrsdaten

Mit Hilfe von retrograden Telekommunikationsverkehrsdaten kann herausgefunden werden, welche Telefonanschlüsse wann miteinander verbunden waren. Als besonders wichtig und wertvoll hat sich die Speicherung von Verkehrsdaten am Beispiel der Bekämpfung des internationalen Terrorismus erwiesen. Die Ausreise radikalisierte Islamisten aus Deutschland und ganz Europa, um sich am „Jihad“ zu beteiligen, ist praktisch immer mit Kontakten zu anderen Islamisten verbunden. Durch die Auswertung von Telekommunikationsverkehrsdaten kann zum Beispiel nachvollzogen werden, mit wem ein mutmaßlicher Terrorist in

Kontakt stand und steht. So können gegebenenfalls auch erhebliche Gefahren im Inland erkannt und abgewendet werden.

III. Ziel

Auf nationaler Ebene erscheint eine (neue) Gesetzesinitiative derzeit angesichts der europa-rechtlichen Vorgaben wenig erfolgversprechend. Unter Anerkennung dieser Realität ist es jedoch die Aufgabe der Union, die Erforderlichkeit der Vorratsdatenspeicherung auf europäischer Ebene fortwährend zu betonen und mit Blick auf die gesamteuropäische Bedrohungslage den Weg zu einer angepassten Rechtslage zu ebnen.

Der dauerhafte Verlust der Vorratsdaten ist im Interesse einer funktionierenden Strafrechtspflege nicht hinnehmbar.