EuGH zur Vorratsdatenspeicherung

Daten über Telefonate, den Standort des Handys oder besuchte Webseiten: Anlasslos darf das nicht gespeichert werden, auch nicht für den Zugriff von Sicherheitsbehörden im Gefahrenfall. Das hat der EuGH kürzlich (erneut) entschieden und die Regelungen zur Vorratsdatenspeicherung im Telekommunikationsgesetz (TKG) für EU-rechtswidrig erklärt. Nun muss der deutsche Gesetzgeber nachbessern. Leitplanken, innerhalb derer die politische Entscheidung gefunden werden muss, ergeben sich aus dem EuGH-Urteil. Wir stellen Ihnen die Entscheidung, ihre Hintergründe und ihre Auswirkungen dar und wagen einen Ausblick auf den deutschen Gesetzentwurf, der inzwischen aus dem Bundesjustizministerium vorliegt.

Schon seit über 5 Jahren sind öffentlich zugängliche Telefondienste und Internetzugangsdienste qua Gesetz dazu verpflichtet, Verkehrs- und Standortdaten ihrer Kunden auf Vorrat allgemein und unterschiedslos zu speichern (§ 176 TKG, § 113b TKG a.F.). Zur Anwendung kamen diese gesetzliche Regelungen jedoch nie, denn die Unternehmen SpaceNet und Telekom Deutschland fochten die Speicherpflicht mit Erfolg vor den deutschen Gerichten an (u.a. OVG Münster, Beschluss vom 22.06.2017, 13 B 238/17). Daraufhin sah die BNetzA insgesamt (gegenüber allen Verpflichteten) – bis zum rechtskräftigen Abschluss eines Hauptsacheverfahrens – von der Durchsetzung der Speicherpflicht ab (siehe Mitteilung der BNetzA).

Nach dem Urteil des EuGH am 20.09.2022 (Urteil vom 20.09.2022, C-793/19, C-794/19 – SpaceNet und Telekom Deutschland) ist nun klar: Die derzeitige Regelung zur Vorratsdatenspeicherung wird auch künftig nicht angewendet werden, da sie gegen Unionsrecht verstößt. Diese Wertung des EuGH muss das BVerwG in seinem jetzt anstehenden Urteil beachten (der EuGH hat in einem Vorabentscheidungsverfahren geurteilt).

Der EuGH bestätigt mit diesem Urteil seine bisherige Rechtsprechung zum Thema Vorratsdatenspeicherung. Insbesondere in seiner Entscheidung betreffend der britischen und der schwedischen Regelungen zur Vorratsdatenspeicherung klärte

der EuGH 2016 grundlegende Rechtsfragen zur Vereinbarkeit der Vorratsdatenspeicherung mit dem Unionsrecht (EuGH, Urteil vom 21.12.2016, C-203/15 und C-698/15 - Tele2 Sverige und Watson u.a.).

Wegen weiterhin bestehender Unklarheiten und inhaltlicher Abweichungen im Vergleich zu den vorgenannten Regelungen sah das BVerwG weiterhin Klärungsbedarf in Bezug auf die deutsche Regelung und entschied sich zur Vorlage (BVerwG, Beschluss vom 25.09.2019, 6 C 12.18 und 6 C 13.18; dazu Pressemitteilung): Die deutsche Regelung erfasse weniger Kommunikationsmittel und nur bestimmte Datenkategorien (ausgenommen sind neben den Inhalten der Kommunikation, u.a. Daten über aufgerufene Internetseiten, Daten von E-Mail-Diensten, siehe § 176 Abs. 5 TKG bzw. § 113b Abs. 5 TKG a.F.). Zudem weise sie eine zeitlich enger begrenzte Speicherfrist (vier bzw. zehn Wochen) auf und enthalte strengere Beschränkungen, die den Schutz der gespeicherten Daten vor Missbrauch und unberechtigtem Zugriff gewährleisten. Außerdem sei nicht eindeutig, ob die Ausführungen des EuGH im Urteil vom 21.12.2016 als generelles Verbot einer anlasslosen Vorratsdatenspeicherung zu verstehen seien. Das BVerwG wies daraufhin, dass ein ausnahmsloses Verbot der anlasslosen Speicherung von Verkehrs- und Standortdaten auf Vorrat die Mitgliedstaaten erheblich beschränken würde, Strafverfolgung und öffentliche Sicherheit eigenständig zu regeln.

Absage an deutsche Regelung

Der EuGH sah die Besonderheiten der deutschen Regelungen, kippte diese im Ergebnis aber dennoch: Eine nationale Regelung wie die im TKG, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen für die *öffentliche* Sicherheit eine allgemeine und unterschiedslose Vorratsdatenspeicherung von Verkehrs- und Standortdaten vorsieht (Rn. 131), ist nicht vereinbar mit dem EU-Recht. Der von der Speicherpflicht erfasste Datensatz sei umfangreich (Rn. 81) und ermögliche auch bei einer Speicherdauer von zehn bzw. vier Wochen „sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden […], und insbesondere die Erstellung eines Profils dieser Personen“ (Rn. 90). Zudem seien die im TKG vorgesehenen Garantien zum Schutz gegen Missbrauch und unberechtigten Zugriff nur geeignet den Eingriff durch Zugang zu den gespeicherten Daten zu beschränken oder zu

beseitigen, nicht jedoch den („naturgemäß schwereren“) Eingriff der Vorratsdatenspeicherung (Rn. 91)

Welche Regelungen wären unionsrechtskonform?

Ein allgemeines Verbot der anlasslosen Vorratsdatenspeicherung sprach der EuGH dagegen nicht aus. Eine **allgemeine und unterschiedslose** Speicherung von Verkehrs- und Standortdaten auf Vorrat kann nach der EuGH-Entscheidung in folgenden Ausnahmefällen und unter Beachtung der genannten Voraussetzungen sowie des Grundsatzes der Verhältnismäßigkeit mit dem Unionsrecht vereinbar sein:

- **Nur zeitlich begrenzt bei ernster Bedrohungslage:** Allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten auf Vorrat nur auf Anordnung zum Schutz der *nationalen Sicherheit*, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden *ernsten Bedrohung* für die nationale Sicherheit gegenübersieht, der Zeitraum, auf den sich die Anordnung erstreckt, auf das absolut Notwendige begrenzt ist und die Anordnung durch ein Gericht oder eine unabhängige Verwaltungsstelle (mit Bindungswirkung) kontrolliert werden kann (Rn. 131, 1. Spiegelstrich).

- Allgemeine und unterschiedslose Speicherung von **IP-Adressen** auf Vorrat zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolute Notwendige begrenzten Zeitraum (Rn. 131, 3. Spiegelstrich).

- Allgemeine und unterschiedslose Speicherung von Daten, die die **Identität der Nutzer elektronischer Kommunikationsmittel** betreffen, auf Vorrat zum Schutz der nationalen Sicherheit, zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit (Rn. 131, 4. Spiegelstrich).

Daneben ist eine **gezielte Vorratsdatenspeicherung** von Verkehrs- und Standortdaten zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit unionsrechtskonform,

sofern die *Speicherung auf Grundlage objektiver und nichtdiskriminierender Kriterien etwa geografisch oder bezogen auf bestimmte Personenkreise eingegrenzt wurde* und sich die Speicherdauer auf ein absolut notweniges Maß begrenzt (Rn. 131, 2. Spiegelstrich).

Schließlich sind nationale Rechtsvorschriften unionsrechtskonform, die es den zuständigen Behörden gestatten, zur Bekämpfung schwerer Kriminalität und, a fortiori, zum Schutz der nationalen Sicherheit Betreibern elektronischer Kommunikationsdienste mittels **Entscheidung** aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten **umgehend zu sichern** (Rn. 131, 5. Spiegelstrich), also einen sog. Quick-Freeze durchzuführen („on the fly").

Zudem schreibt der EuGH (in Fortführung seiner bisherigen Rechtsprechung) vor: **Klare und präzise Regeln** müssen sicherstellen, dass die geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen (Rn. 131).

Was kommt nun?

Die Leitplanken hat der EuGH damit vorgegeben. Nachbessern muss der deutsche Gesetzgeber in jedem Fall. Er kann die Möglichkeiten, die das EuGH-Urteil offenlässt, voll ausschöpfen oder eine weniger eingriffsintensive Regelung wählen.

Das BMJ hat sich nun für die wohl am wenigsten eingriffsintensive Option entschieden, das sog. Quick-Freeze-Verfahren. Dazu hat das BMJ nun auch einen Gesetzesentwurf vorgelegt. Dieses Verfahren sieht vor, dass die bei den Anbietern von Telekommunikationsdiensten ohnehin bereits vorhandenen und künftig anfallenden Verkehrsdaten gesichert werden („Einfrieren"), wenn dies zur Verfolgung von erheblichen Straftaten beitragen kann. Informationen, die in den Telekommunikationssystemen vorliegen, müssen dann technisch so erhoben und abgelegt werden, dass ein späterer Zugriff möglich ist. Diese „Einfrieren" erfolgt „on the fly", d.h. bei einem entsprechenden Anlass fordert eine befugte Behörde den Telekommunikationsanbieter auf, zu sichern, welcher Person zum konkreten Zeitpunkt eine IP-Adresse zugeordnet ist, welche Verkehrs- oder Standortdaten u.ä.

Im ersten Schritt wird dabei nur die Sicherung der Daten angeordnet, ohne direkten Zugriff (§ 100g Abs. 1 StPO). Im zweiten Schritt können Behörden dann die Herausgabe fordern und damit auch auf die Daten zugreifen (§ 100g Abs. 1, 3 StPO). So soll verhindert werden, dass ermittlungsrelevante Daten gelöscht werden (mussten), bevor ausreichend Beweise vorlagen, um als Ermittlungsbehörde tatsächlich Zugriff auf diese Daten erhalten zu können. Abgesichert wird so aber, dass keine anlasslose Vorratsdatenspeicherung, unterschiedslos, erfolgt, sondern nur im Fall hinreichend konkreter Anhaltspunkte.

Die technischen Vorkehrungen für die Durchführung von Quick-Freeze-Verfahren haben Telekommunikationsanbieter auf eigene Kosten vorzusehen, wie auch bisher schon. Erreichen sie konkrete Anfragen, werden diese Kosten erstattet.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de