parleu2020.de

Deutscher Bundestag
Fachbereich Europa

Aktueller Begriff Europa
Die Vorratsdatenspeicherung in der Rechtsprechung des EuGH

Der Europäische Gerichtshof (EuGH) hat sich am 6. Oktober 2020 in zwei Entscheidungen in der Rs. C-623/17 (*Privacy International*) und den verbundenen Rs. C-511/18, C-512/18 und C-520/18 (*La Quadrature du Net u.a.*) mit der Vorratsdatenspeicherung (VDS) befasst. Die von britischen, französischen und belgischen Gerichten initiierten Vorabentscheidungsverfahren dienten der Klärung zentraler Fragen zur Richtlinie 2002/58/EG (sog. ePrivacy-Richtlinie) und der Charta der Grundrechte der Europäischen Union (GRC). Der EuGH bestätigt seine bisherige Rechtsprechung, die eine allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten einem grundsätzlichen Verbot unterwirft, präzisiert jedoch auch mögliche Ausnahmen.

Hintergrund: Die VDS wird seit vielen Jahren auf nationaler und europäischer Ebene kontrovers diskutiert. Mit Urteil vom 8. April 2014 in den verbundenen Rs. C-293 und C-594/12 (*Digital Rights Ireland*) erklärte der EuGH die in der Richtlinie 2006/24/EG enthaltene Verpflichtung zur Vorratsdatenspeicherung als mit Art. 7 und 8 GRC unvereinbar. Die Eingriffe in das Recht auf Achtung des Privat- und Familienlebens (Art. 7 GRC) und in das Recht auf Schutz personenbezogener Daten (Art. 8 GRC) seien von großem Ausmaß und besonderer Schwere, ohne dass sie Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt – etwa durch eine klare Begrenzung des Personenkreises, der Speicherfristen, der Zugangsvoraussetzungen, sowie ausreichende Verfahrensgarantien für die Betroffenen.

Der EuGH setzte diese Linie im Urteil vom 21. Dezember 2016 in den verbundenen Rs. C-203/15 und C-698/15 (Tele2 Sverige u.a.) fort. In diesem Vorabentscheidungsverfahren befasste er sich mit dem Geltungsbereich und der Reichweite des Art. 15 Abs.1 der ePrivacy-Richtlinie, der Ausnahmen vom Grundsatz der Vertraulichkeit der Kommunikation vorsieht. Nach einer Klarstellung, dass auch mitgliedsstaatliche Regelungen zur VDS in den Anwendungsbereich des Unionsrechts fallen und sich daher an der GRC messen lassen müssen, bekräftigt er das grundsätzliche Verbot der allgemeinen und unterschiedslosen Speicherung von Verkehrs- und Standortdaten. Ausnahmen könnten zwar zur Verfolgung schwerer Straftaten zulässig sein, unterlägen aber wegen der Intensität des Eingriffs in die Gewährleistungen der GRC einer strikten Verhältnismäßigkeitsprüfung. Zwingend notwendig seien auch hier Maßnahmen zur Begrenzung des potenziell betroffenen Personenkreises durch objektive Kriterien, Vorschriften zur Sicherheit und zum Schutz der gespeicherten Daten und eine vorherige, unabhängige Kontrolle vor dem Datenabruf durch ein Gericht oder eine unabhängige Verwaltungsbehörde.

Aktuelle Entscheidungen: In den Urteilen vom 6. Oktober 2020, für die noch keine deutschen Übersetzungen vorliegen, hält der EuGH an seiner Rechtsprechung zur VDS fest und sieht den Anwendungsbereich der ePrivacy-Richtlinie sowohl für Speicherpflichten der Telekommunikationsunternehmen als auch für Abrufbefugnisse durch Sicherheitsbehörden als eröffnet an.

Auch weiterhin soll gelten, dass grundsätzlich eine allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten mit dem Unionsrecht unvereinbar ist, da sich der Eingriff in die entsprechenden Grundrechte nicht auf das absolut Notwendige beschränkt. Neben Art. 7 und Art. 8 GRC wird zudem eine Gefahr für die Meinungsfreiheit aus Art. 11 GRC hervorgehoben:

Nr. 05/20 (22. Oktober 2020) © 2020 Deutscher Bundestag

Verfasser: Gepr. Rk Paul Hothneier; Dr. Roland Derksen
Fachbereich Europa (PE 6), Telefon: +49 30 227-33614, vorzimmer.pe6@bundestag.de

Durch das Gefühl der ständigen Überwachung könnten Bürgerinnen und Bürger darin beeinträchtigt werden, ihre Meinung uneingeschränkt zu äußern.

Aus Art. 15 Abs. 1 ePrivacy-Richtlinie folgten allerdings wichtige Ausnahmen von diesem Grundsatz: Bei einer tatsächlichen **ernsthaften Bedrohung für die nationale Sicherheit,** die gegenwärtig oder vorhersehbar ist,[1] bleibe ein enger Spielraum für eine allgemeine und unterschiedslose Speicherung solcher Daten. Diese Speicherung und der Abruf der Daten müsse aber durch zeitliche Begrenzungen und umfassende gerichtliche Kontrollmöglichkeiten verhältnismäßig ausgestaltet werden. Bei der **Verfolgung schwerer Straftaten** soll ebenso eine verhältnismäßige Ausgestaltung der gezielten Speicherung von Daten verdächtiger Personengruppen anknüpfend an die Tele2-Entscheidung aus dem Jahre 2016 möglich sein, sofern die Speicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist.

Beispielhaft ist auch auf die **Speicherung von IP-Adressen** als weitere Ausnahme hinzuweisen, welche der EuGH als eine weniger intensive Grundrechtsbeeinträchtigung einstuft. Die IP-Adresse erleichtere zwar die Zuordnung von Daten zu einer Person, gebe jedoch nur in begrenzterem Maße darüber Aufschluss, mit wem diese Person kommuniziert und in sonstiger Weise in Verbindung getreten ist. Die Gefahr, dass auf diesem Wege ein umfassendes Profil über Nutzerinnen und Nutzer erstellt werden könne, sei deshalb als geringer anzusehen. Auch hier sollen allerdings die strikten Voraussetzungen des Grundsatzes der Verhältnismäßigkeit einzuhalten sein, beispielsweise durch Speicherfristen und hinreichende gerichtliche Kontrollmöglichkeiten. Darüber hinaus sind unionsrechtskonforme Ausgestaltungen nationaler Gesetze denkbar, die eine **verlängerte Speicherung** bereits gesammelter Daten (etwa zu Abrechnungszwecken) von Telekommunikationsdienstleistern ermöglichen. Sie sollen in konkreten Verdachtsmomenten dazu beitragen, auf Gefährdungen der nationalen Sicherheit reagieren zu können oder Ermittlungen schwerer Straftaten zu erleichtern. Auch hier müssen objektive und nicht diskriminierende Kriterien den betroffenen Personenkreis abgrenzen, um den Abruf durch die Sicherheitsbehörden auf das absolut Notwendige zu beschränken.

Abschließend stellt der EuGH fest, dass das Unionsrecht zwar grundsätzlich keine Auswirkungen auf das mitgliedstaatliche Strafverfahrensrecht habe, aber Informationen, deren Speicherung nach den vorgenannten Maßstäben als unionsrechtswidrig gelten, von nationalen Gerichten wegen des Grundsatzes der effektiven Durchsetzung des Unionsrechts nicht berücksichtigt werden dürfen.

Ausblick: Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I, S. 2218) diente der Einführung einer VDS in Deutschland. Die Bundesnetzagentur sieht derzeit nach einigen verwaltungsgerichtlichen Entscheidungen in Anbetracht der unklaren Rechtslage von der Verfolgung etwaiger Verstöße gegen Speicherpflichten nach dem durch dieses Gesetz novellierten Telekommunikationsgesetz ab. Inzwischen hat das Bundesverwaltungsgericht sich mit einem Vorabentscheidungsersuchen zu der deutschen Regelung zur VDS an den EuGH gewandt (BVerwG, Beschl. v. 25.9.2019, Az. 6 C 12.18). Wie sich die aktuellen Entscheidungen in den Fällen Privacy International und La Quadrature du Net auf dieses Verfahren auswirken werden, bleibt abzuwarten.

Quellen

EuGH, Urt. v. 8.4.2014, verb. Rs. C-293/12 und C-594/12 (*Digital Rights Ireland*)
EuGH, Urt. v. 21.12.2016, verb. Rs. C-203/15 und C-698/15 (*Tele2 Sverige u.a.*)
EuGH, Urt. v. 6.10.2020, Rs. C-623/17 (*Privacy International*) und verb. Rs. C-511/18, C-512/18 und C-520/18 (*La Quadrature du Net u.a*).

1 In der englischen Fassung des Urteils: „serious threat to national security that is shown to be genuine and present or foreseeable".