Datenschutz

C-793/19 und C-794/19 - EuGH bestätigt: Vorratsdatenspeicherung ist illegal

Zur Bekämpfung schwerer Kriminalität können die Mitgliedstaaten jedoch unter strikter Beachtung des Grundsatzes der Verhältnismäßigkeit insbesondere eine gezielte Vorratsspeicherung und/oder umgehende Sicherung solcher Daten sowie eine allgemeine und unterschiedslose Speicherung von IP-Adressen vorsehen.

SpaceNet und Telekom Deutschland erbringen in Deutschland öffentlich zugängliche Internetzugangsdienste; Telekom Deutschland erbringt darüber hinaus öffentlich zugängliche Telefondienste. Beide fochten vor den deutschen Gerichten die ihnen durch das deutsche Telekommunikationsgesetz (TKG) auferlegte Pflicht an, ab dem 1. Juli 2017 Verkehrs- und Standortdaten betreffend die Telekommunikation ihrer Kunden auf Vorrat zu speichern.

Abgesehen von bestimmten Ausnahmen verpflichtet das TKG die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste – insbesondere zur Verfolgung schwerer Straftaten oder zur Abwehr einer konkreten Gefahr für die nationale Sicherheit – zu einer allgemeinen und unterschiedslosen Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten der Endnutzer dieser Dienste für eine Dauer von mehreren Wochen.

Das Bundesverwaltungsgericht (Deutschland) möchte wissen, ob das Unionsrecht in seiner Auslegung durch den Gerichtshof[1] solchen nationalen Rechtsvorschriften entgegensteht.

Seine Zweifel beruhen insbesondere darauf, dass die nach dem TKG vorgesehene Speicherpflicht weniger Daten und eine kürzere Speicherungsfrist (vier bzw. zehn Wochen) betrifft, als sie die nationalen Regelungen vorsahen, um die es in den Rechtssachen ging, in denen die vorangegangenen Urteile ergangen sind. Diese Besonderheiten verringern nach Ansicht des Bundesverwaltungsgerichts die Möglichkeit, dass aus den gespeicherten Daten sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert worden seien, gezogen würden. Außerdem gewährleiste das TKG, dass die auf Vorrat gespeicherten Daten wirksam vor den Risiken eines Missbrauchs und eines unberechtigten Zugangs geschützt seien.

Mit seinem Urteil von heute bestätigt der Gerichtshof seine bisherige Rechtsprechung.

Er antwortet dem Bundesverwaltungsgericht, dass das Unionsrecht nationalen Rechtsvorschriften entgegensteht, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen.

Dagegen steht das Unionsrecht nationalen Rechtsvorschriften nicht entgegen, die

- es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht. Eine solche Anordnung kann durch ein Gericht oder eine unabhängige Verwaltungsstelle kontrolliert werden und darf nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergehen;
- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;
- für dieselben Zwecke einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;
- zum Schutz der nationalen Sicherheit, zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;
- es zur Bekämpfung schwerer Kriminalität und, a fortiori, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Solche nationalen Rechtsvorschriften müssen außerdem durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.

In Bezug auf das TKG stellt der Gerichtshof fest, dass aus der Vorlageentscheidung hervorgeht, dass die durch dieses Gesetz begründete Pflicht zur Vorratsspeicherung insbesondere die Daten betrifft, die erforderlich sind, um die Quelle und den Adressaten einer Nachricht, Datum und Uhrzeit von Beginn und Ende der Verbindung oder, im Fall der Übermittlung von Kurz-, Multimedia- oder ähnlichen Nachrichten, die Zeitpunkte der Versendung und des Empfangs der Nachricht sowie, im Fall der mobilen Nutzung, die Bezeichnung der Funkzellen, die vom Anrufer und vom Angerufenen bei Beginn der Verbindung genutzt wurden, zu identifizieren.

Im Rahmen der Bereitstellung von Internetzugangsdiensten bezieht sich die Pflicht zur Vorratsspeicherung u. a. auf die dem Teilnehmer zugewiesene IP-Adresse, Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen IP-Adresse und, im Fall der mobilen Nutzung, die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle. Die Daten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben, werden ebenfalls gespeichert.

Zwar werden die Daten betreffend E-Mail-Dienste nicht von der in der im TKG vorgesehenen Pflicht zur Vorratsspeicherung erfasst, jedoch stellen sie auch nur einen Bruchteil der in Rede stehenden Daten dar. Außerdem werden u. a. Daten von Nutzern gespeichert, die dem Berufsgeheimnis unterliegen, wie beispielsweise Rechtsanwälte, Ärzte und Journalisten.

Die im TKG vorgesehene Pflicht zur Vorratsspeicherung erstreckt sich somit auf einen umfangreichen Satz von Verkehrs- und Standortdaten, der im Wesentlichen den Datensätzen entspricht, die zu den vorgenannten früheren Urteilen geführt haben.

Ein solcher Satz von Verkehrs- und Standortdaten, die zehn bzw. vier Wochen lang gespeichert werden, kann aber sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden – etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren –, und insbesondere die Erstellung eines Profils dieser Personen ermöglichen.

In Bezug auf die im TKG vorgesehenen Garantien, die die gespeicherten Daten gegen Missbrauchsrisiken und vor jedem unberechtigten Zugang schützen sollen, weist der Gerichtshof darauf hin, dass die Vorratsspeicherung dieser Daten und der Zugang zu ihnen unterschiedliche Eingriffe in Grundrechte der Betroffenen darstellen, die eine gesonderte Rechtfertigung erfordern.

Daraus folgt, dass nationale Rechtsvorschriften, die die vollständige Einhaltung der Voraussetzungen gewährleisten, die sich im Bereich des Zugangs zu auf Vorrat gespeicherten Daten aus der Rechtsprechung ergeben, naturgemäß den schwerwiegenden Eingriff in die Rechte der Betroffenen, der sich aus der allgemeinen Vorratsspeicherung dieser Daten ergeben würde, weder beschränken noch beseitigen können.

EuGH-Urteil vom 20. Sept 2022; C-793/19 SpaceNet und C-794/19 Telekom Deutschland; EuGH PM 156/2022

---

1 Siehe u. a. Urteile vom Urteile vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20 (siehe auch EuGH PM 58/2022), sowie vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18 (siehe auch EuGH PM 123/2020).

E-Learning Datenschutz

Datenschutz praktische Lektion

Zur Buchung (EUR 7,00 / 1 Monat)

7 Min Datenschutz juristi.e-Seminar

Aus- und Weiterbildung