



Presse und Information

Gerichtshof der Europäischen Union

**PRESSEMITTEILUNG Nr. 145/16**

Luxemburg, den 21. Dezember 2016

Urteil in den verbundenen Rechtssachen C-203/15,  
Tele2 Sverige AB / Post- och telestyrelsen, und C-698/15,  
Secretary of State for the Home Department / Tom Watson u. a

## **Die Mitgliedstaaten dürfen den Betreibern elektronischer Kommunikationsdienste keine allgemeine Verpflichtung zur Vorratsdatenspeicherung auferlegen**

*Das Unionsrecht untersagt eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten. Es steht den Mitgliedstaaten aber frei, vorbeugend eine gezielte Vorratsspeicherung dieser Daten zum alleinigen Zweck der Bekämpfung schwerer Straftaten vorzusehen, sofern eine solche Speicherung hinsichtlich der Kategorien von zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Speicherung auf das absolut Notwendige beschränkt ist. Der Zugang der nationalen Behörden zu den auf Vorrat gespeicherten Daten muss von Voraussetzungen abhängig gemacht werden, zu denen insbesondere eine vorherige Kontrolle durch eine unabhängige Stelle und die Vorratsspeicherung der Daten im Gebiet der Union gehören*

Mit dem Urteil Digital Rights Ireland von 2014<sup>1</sup> hat der Gerichtshof die Richtlinie über die Vorratsspeicherung von Daten<sup>2</sup> für ungültig erklärt, weil der Eingriff in die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten durch die mit dieser Richtlinie vorgeschriebene allgemeine Verpflichtung zur Vorratsspeicherung von Verkehrs- und Standortdaten nicht auf das absolut Notwendige beschränkt war.

Im Anschluss an dieses Urteil ist der Gerichtshof mit zwei Rechtssachen befasst worden, in denen es um die den Betreibern elektronischer Kommunikationsdienste in Schweden und im Vereinigten Königreich auferlegte allgemeine Verpflichtung geht, Daten elektronischer Kommunikationsvorgänge, deren Vorratsspeicherung in der für ungültig erklärten Richtlinie vorgesehen war, auf Vorrat zu speichern.

Am Tag nach der Verkündung des Urteils Digital Rights Ireland teilte das Telekommunikationsunternehmen Tele2 Sverige der schwedischen Überwachungsbehörde für Post und Telekommunikation mit, dass es die Vorratsspeicherung von Daten einstellen werde und beabsichtige, die bereits gespeicherten Daten zu löschen (Rechtssache C-203/15). Nach schwedischem Recht sind die Betreiber elektronischer Kommunikationsdienste nämlich verpflichtet, systematisch und kontinuierlich, und dies ohne jede Ausnahme, sämtliche Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel zu speichern.

In der Rechtssache C-698/15 klagten Herr Tom Watson, Herr Peter Brice und Herr Geoffrey Lewis gegen die britischen Regelung über die Vorratsspeicherung von Daten, die den Innenminister ermächtigt, die Betreiber öffentlicher Telekommunikationsdienste zu verpflichten, sämtliche Kommunikationsdaten für bis zu zwölf Monate auf Vorrat zu speichern, wobei die Speicherung des Inhalts der Kommunikationsvorgänge ausgeschlossen ist.

Der Gerichtshof ist vom Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm, Schweden) und vom Court of Appeal (England and Wales) (Civil Division) (Rechtsmittelgerichtshof für England

<sup>1</sup> Urteil des Gerichtshofs vom 8. April 2014, Digital Rights Ireland u. a. (verbundene Rechtssachen [C-293/12 und C-594/12](#), vgl. Pressemitteilung [Nr. 54/14](#)).

<sup>2</sup> Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. L 105, S. 54).

und Wales, Vereinigtes Königreich) gefragt worden, ob nationale Regelungen, die den Betreibern eine allgemeine Verpflichtung zur Vorratsspeicherung von Daten auferlegen und den zuständigen nationalen Behörden den Zugang zu den gespeicherten Daten ermöglichen, ohne dass dieser Zugang auf die Zwecke der Bekämpfung schwerer Straftaten beschränkt wäre und einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde unterworfen wäre, mit dem Unionsrecht – im vorliegenden Fall der „Datenschutzrichtlinie für elektronische Kommunikation“<sup>3</sup> im Licht der EU-Grundrechtecharta<sup>4</sup> – vereinbar sind.

In seinem heutigen Urteil **antwortet der Gerichtshof, dass das Unionsrecht einer nationalen Regelung entgegensteht, die eine allgemeine und unterschiedslose Speicherung von Daten vorsieht.**

Der Gerichtshof bestätigt zunächst, dass **die in Rede stehenden nationalen Rechtsvorschriften in den Geltungsbereich der Richtlinie fallen.** Denn die mit der Datenschutzrichtlinie garantierte Vertraulichkeit elektronischer Kommunikationen und der Verkehrsdaten gilt für Maßnahmen sämtlicher anderer Personen als der Nutzer, unabhängig davon, ob es sich um private Personen oder Einrichtungen oder um staatliche Einrichtungen handelt.

Sodann stellt der Gerichtshof fest, dass die Datenschutzrichtlinie zwar den Mitgliedstaaten erlaubt, die Tragweite der grundsätzlichen Verpflichtung, die Vertraulichkeit der Kommunikation und der damit verbundenen Verkehrsdaten zu gewährleisten, einzuschränken, sie es aber nicht zu rechtfertigen vermag, dass die Ausnahme von dieser grundsätzlichen Verpflichtung und insbesondere von dem mit dieser Richtlinie aufgestellten Verbot der Speicherung dieser Daten zur Regel wird.

Der Gerichtshof weist außerdem auf seine ständige Rechtsprechung hin, wonach der Schutz des Grundrechts auf Achtung des Privatlebens verlangt, dass sich die **Ausnahmen** vom Schutz personenbezogener Daten **auf das absolut Notwendige beschränken.** Der Gerichtshof wendet diese Rechtsprechung sowohl auf die Regeln über die Vorratsdatenspeicherung als auch auf die Regeln über den Zugang zu den gespeicherten Daten an.

**In Bezug auf die Vorratsspeicherung** stellt der Gerichtshof fest, dass aus der Gesamtheit der gespeicherten Daten **sehr genaue Schlüsse auf das Privatleben der Personen,** deren Daten auf Vorrat gespeichert wurden, **gezogen werden können.**

**Der Grundrechtseingriff, der mit einer nationalen Regelung einhergeht, die eine Speicherung von Verkehrs- und Standortdaten vorsieht, ist somit als besonders schwerwiegend anzusehen.** Der Umstand, dass die Vorratsspeicherung der Daten vorgenommen wird, ohne dass die Nutzer elektronischer Kommunikationsdienste darüber informiert werden, ist geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist. Deshalb **vermag allein die Bekämpfung schwerer Straftaten einen solchen Grundrechtseingriff zu rechtfertigen.**

Der Gerichtshof weist darauf hin, dass eine **Regelung, die eine allgemeine und unterschiedslose Vorratsdatenspeicherung vorsieht, keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit verlangt und sich** insbesondere nicht auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, beschränkt. **Eine solche nationale Regelung überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es die Richtlinie im Licht der Grundrechtecharta verlangt.**

---

<sup>3</sup> Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201, S. 37) in der Fassung der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. L 337, S. 11).

<sup>4</sup> Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union.

Der Gerichtshof stellt jedoch klar, dass **die Datenschutzrichtlinie einer nationalen Regelung nicht entgegensteht**, die zur Bekämpfung schwerer Straftaten **eine gezielte Vorratsspeicherung von Daten ermöglicht, sofern diese Vorratsspeicherung** hinsichtlich der Kategorien von zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Speicherdauer **auf das absolut Notwendige beschränkt ist**. Dem Gerichtshof zufolge **muss jede nationale Regelung, die derartiges vorsieht, klar und präzise sein und hinreichende Garantien enthalten**, um die Daten vor Missbrauchsrisiken zu schützen. Die betreffende Regelung muss angeben, unter welchen Umständen und Voraussetzungen eine Maßnahme der Vorratsspeicherung von Daten vorbeugend getroffen werden darf, um so zu gewährleisten, dass der Umfang dieser Maßnahme in der Praxis tatsächlich auf das absolut Notwendige beschränkt ist. Eine solche Regelung muss insbesondere auf objektive Anknüpfungspunkte gestützt sein, die es ermöglichen diejenigen Personen zu erfassen, deren Daten geeignet sind, einen Zusammenhang mit schweren Straftaten aufzuweisen, zur Bekämpfung schwerer Straftaten beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern.

Was den **Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten** betrifft, bekräftigt der Gerichtshof, dass sich die betreffende nationale Regelung nicht darauf beschränken darf, zu verlangen, dass der Zugang einem der in der Datenschutzrichtlinie genannten Zwecke dienen muss – auch wenn es sich bei diesem Zweck um die Bekämpfung schwerer Straftaten handelt –, sondern außerdem die materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten festzulegen hat. Die nationale Regelung muss sich **bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugang zu den Daten zu gewähren ist, auf objektive Kriterien** stützen. Zum Zweck der Bekämpfung von Straftaten darf Zugang grundsätzlich nur zu Daten von Personen gewährt werden, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein. Allerdings könnte in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristischen Aktivitäten bedroht sind, der Zugang zu Daten anderer Personen ebenfalls gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten im konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten könnten.

Zudem **ist es** nach Auffassung des Gerichtshofs **unerlässlich, dass der Zugang zu den auf Vorrat gespeicherten Daten grundsätzlich, außer in Eilfällen, einer vorherigen Kontrolle** entweder durch ein Gericht oder eine unabhängige Stelle **unterworfen wird**. Außerdem müssen die zuständigen nationalen Behörden, denen Zugang zu den gespeicherten Daten gewährt wurde, die betroffenen Personen davon in Kenntnis setzen.

In Anbetracht der Menge an gespeicherten Daten, ihres sensiblen Charakters und der Gefahr eines unberechtigten Zugangs **muss die nationale Regelung vorsehen, dass die Daten im Gebiet der Union zu speichern sind** und nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten sind.

---

**HINWEIS:** Im Wege eines Vorabentscheidungsersuchens können die Gerichte der Mitgliedstaaten in einem bei ihnen anhängigen Rechtsstreit dem Gerichtshof Fragen nach der Auslegung des Unionsrechts oder nach der Gültigkeit einer Handlung der Union vorlegen. Der Gerichtshof entscheidet nicht über den nationalen Rechtsstreit. Es ist Sache des nationalen Gerichts, über die Rechtssache im Einklang mit der Entscheidung des Gerichtshofs zu entscheiden. Diese Entscheidung des Gerichtshofs bindet in gleicher Weise andere nationale Gerichte, die mit einem ähnlichen Problem befasst werden.

---

*Zur Verwendung durch die Medien bestimmtes nichtamtliches Dokument, das den Gerichtshof nicht bindet.*

*Der [Volltext](#) des Urteils wird am Tag der Verkündung auf der Curia-Website veröffentlicht.*

*Pressekontakt: Hartmut Ost ☎ (+352) 4303 3255*

*Filmaufnahmen von der Verkündung des Urteils sind verfügbar über  
„[Europe by Satellite](#)“ ☎ (+32) 2 2964106*