



**Generalanwalt Saugmandsgaard Øe schlägt dem Gerichtshof vor zu entscheiden,
dass auch Straftaten, die nicht von besonderer Schwere sind, einen Zugang zu
grundlegenden Metadaten der elektronischen Kommunikation rechtfertigen können,
vorausgesetzt, dieser Zugang führt nicht zu einer schwerwiegenden
Beeinträchtigung des Privatlebens**

Die spanische Kriminalpolizei beantragte beim Ermittlungsrichter, ihr im Rahmen einer Untersuchung wegen des Raubs einer Brieftasche und eines Mobiltelefons Zugang zu den Identifikationsdaten der Nutzer der Telefonnummern zu gewähren, die in einem Zeitraum von zwölf Tagen ab dem Tag des Raubs mit dem entwendeten Mobiltelefon angerufen wurden. Der Ermittlungsrichter wies diesen Antrag u. a. mit der Begründung zurück, dass der den strafrechtlichen Ermittlungen zugrunde liegende Sachverhalt keine „schwere“ Straftat – d. h. nach spanischem Recht eine mit einer Freiheitsstrafe von mehr als fünf Jahren bedrohte Straftat – darstelle und der Zugang zu Identifikationsdaten in Spanien nur bei dieser Art von Straftaten möglich sei. Das Ministerio Fiscal (Staatsanwaltschaft) legte gegen diese Entscheidung bei der Audiencia Provincial de Tarragona (Regionalgericht Tarragona, Spanien) Berufung ein.

Die Datenschutzrichtlinie für elektronische Kommunikation¹ sieht vor, dass die Mitgliedstaaten die Rechte der Bürger beschränken können, sofern eine solche Beschränkung für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.

Der Gerichtshof hat in seinen Urteilen Digital Rights² und Tele2 Sverige³ den Begriff der „schweren Straftaten“ verwendet, um die Rechtmäßigkeit und die Verhältnismäßigkeit eines Eingriffs in das Recht auf Achtung des Privat- und Familienlebens und das Recht auf Schutz personenbezogener

¹ 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. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung.

² Urteil vom 8. April 2014, Digital Rights Ireland ([C-293/12 und C-594/12](#), siehe Pressemitteilung [Nr. 54/14](#)). Mit diesem Urteil hat der Gerichtshof die 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. 2006, L 105, S. 54) für ungültig erklärt.

³ Urteil vom 21. Dezember 2016, Tele2 Sverige ([C-203/15 und C-698/15](#), siehe Pressemitteilung [Nr. 145/16](#)). In diesem Urteil hat der Gerichtshof entschieden, dass das Unionsrecht zum einen „einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht“, und zum anderen „einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind“.

Daten zu beurteilen, die beide in der Charta der Grundrechte der Europäischen Union verankert sind.

Die Audiencia Provincial de Tarragona weist darauf hin, dass der spanische Gesetzgeber nach dem Erlass der Entscheidung des Ermittlungsrichters zwei alternative Kriterien für die Bestimmung der Schwere einer Straftat eingeführt habe, bei der die Speicherung und die Weitergabe von personenbezogenen Daten zulässig seien. Das erste Kriterium sei ein materielles Kriterium, das an das Vorliegen terroristischer Straftaten und von Straftaten, die im Rahmen einer kriminellen Gruppe oder Organisation begangen würden, anknüpfe. Das zweite Kriterium sei ein normativ-formales Kriterium, nämlich eine angedrohte Mindestfreiheitsstrafe von drei Jahren. Das spanische Gericht betont, dass diese Mindeststrafe eine deutliche Mehrheit der Straftatbestände umfassen könne. Die Audiencia Provincial de Tarragona möchte daher vom Gerichtshof wissen, wie die Schwelle der Schwere der Straftaten zu bestimmen ist, ab der beim Zugang der zuständigen nationalen Behörden zu von Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten im Hinblick auf die genannten Urteile ein Grundrechtseingriff gerechtfertigt sein kann.

In seinen Schlussanträgen vom heutigen Tag stellt Generalanwalt Henrik Saugmandsgaard Øe zunächst fest, dass eine Maßnahme wie die im vorliegenden Fall von der Kriminalpolizei beantragte einen Eingriff in das Recht auf Achtung des Privat- und Familienlebens und das Recht auf Schutz personenbezogener Daten darstelle. Allerdings **habe der Gerichtshof in den Urteilen Digital Rights und Tele2 einen Zusammenhang zwischen der Schwere des festgestellten Eingriffs und der Schwere der Gründe, die diesen Eingriff rechtfertigen könnten, hergestellt.** Um auf der Ebene der Rechtfertigung eines solchen Eingriffs das Vorliegen einer „schweren Straftat“ zu fordern, die es erlaube, vom Grundsatz der Vertraulichkeit der elektronischen Kommunikation abzuweichen, müsse es sich somit **um einen schweren Eingriff handeln. An diesem Merkmal fehlt es nach Ansicht des Generalanwalts im vorliegenden Fall.**

Der Generalanwalt führt weiter aus, dass die Art des in dieser Rechtssache in Rede stehenden Eingriffs sich von den Eingriffen unterscheide, um die es in den beiden genannten Urteilen gegangen sei. **Es handle sich nämlich um eine gezielte Maßnahme**, die auf die Möglichkeit eines Zugangs der zuständigen Behörden für die Zwecke einer strafrechtlichen Ermittlung zu Daten gerichtet sei, die von Dienstleistern für wirtschaftliche Zwecke gespeichert würden, und die ausschließlich die Identität (Name, Vorname und eventuell die Anschrift) einer begrenzten Gruppe von Teilnehmern oder Nutzern eines bestimmten Kommunikationsmittels betreffe, nämlich jene, deren Telefonnummer mit dem Mobiltelefon, dessen Diebstahl Gegenstand der Ermittlungen sei, **in einem begrenzten Zeitraum**, nämlich etwa zwölf Tagen, angerufen worden sei. **Nach Ansicht des Generalanwalts sind die möglichen schädlichen Folgen für die von dem fraglichen Antrag auf Zugang betroffenen Personen sowohl moderat als auch begrenzt**, da sie nicht für eine Verbreitung in der Öffentlichkeit bestimmt seien und die den Polizeibehörden eingeräumte Zugangsmöglichkeit von Verfahrensgarantien eingeeht sei, da sie einer richterlichen Kontrolle unterliege. **Folglich sei der sich aus der Übermittlung dieser Daten über die Identität ergebende Eingriff nicht besonders schwer**, weil diese Daten unter diesen besonderen Umständen die Intimität des Privatlebens der Betroffenen nicht unmittelbar und stark beeinträchtigten.

Der Generalanwalt weist darauf hin, dass nach der Richtlinie eine Abweichung vom Grundsatz der Vertraulichkeit der elektronischen Kommunikation durch das Ziel des Allgemeininteresse gerechtfertigt sein könne, Straftaten zu verhüten und zu verfolgen, ohne dass deren Art näher bezeichnet würde. Die Straftaten, die die betreffende einschränkende Maßnahme rechtfertigten, müssten somit nicht zwingend als „schwer“ im Sinne der Urteile Digital Rights und Tele2 zu qualifizieren sein. Nach Ansicht des Generalanwalts **müssen nur dann, wenn der erlittene Eingriff besonders schwer ist, auch die Straftaten, die einen solchen Eingriff rechtfertigen, besonders schwer sein. Hingegen könnten im Fall eines nicht schweren Eingriffs (d. h., wenn die Daten, deren Übermittlung beantragt wird, das Privatleben nicht schwerwiegend beeinträchtigen) auch Straftaten, die nicht von besonderer Schwere seien, einen solchen Eingriff (d. h. den Zugang zu den begehrten Daten) rechtfertigen.**

Konkret vertritt der Generalanwalt die Auffassung, dass **das Unionsrecht dem Zugang der zuständigen Behörden zu Identifikationsdaten, die im Besitz von Anbietern von Kommunikationsdiensten seien, nicht entgegenstehe, wenn diese Daten es gestatten, die möglichen Täter einer Straftat, die nicht schwer sei, aufzufinden. Der Generalanwalt schließt daraus, dass die im vorliegenden Fall von der Kriminalpolizei beantragte Maßnahme im Licht der Richtlinie einen Eingriff in die durch die Richtlinie und die Charta gewährleisteten Grundrechte darstelle, der keinen ausreichenden Schweregrad erreiche, um einen solchen Zugang auf die Fälle zu beschränken, in denen die betreffende Straftat schwer sei.**

HINWEIS: Die Schlussanträge des Generalanwalts sind für den Gerichtshof nicht bindend. Aufgabe des Generalanwalts ist es, dem Gerichtshof in völliger Unabhängigkeit einen Entscheidungsvorschlag für die betreffende Rechtssache zu unterbreiten. Die Richter des Gerichtshofs treten nunmehr in die Beratung ein. Das Urteil wird zu einem späteren Zeitpunkt verkündet.

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](#) der Schlussanträge wird am Tag der Verlesung 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*