Sammlung der Rechtsprechung

URTEIL DES GERICHTSHOFS (Große Kammer)

2. Oktober 2018*

„Vorlage zur Vorabentscheidung – Elektronische Kommunikation – Verarbeitung personenbezogener Daten – Richtlinie 2002/58/EG – Art. 1 und 3 – Geltungsbereich – Vertraulichkeit der elektronischen Kommunikation – Schutz – Art. 5 und 15 Abs. 1 – Charta der Grundrechte der Europäischen Union – Art. 7 und 8 – Bei der Bereitstellung elektronischer Kommunikationsdienste verarbeitete Daten – Zugang nationaler Behörden zu Daten für Ermittlungszwecke – Schwelle der Schwere einer Straftat, ab der ein Zugang zu den Daten gerechtfertigt sein kann“

In der Rechtssache C-207/16

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht von der Audiencia Provincial de Tarragona (Regionalgericht Tarragona, Spanien) mit Entscheidung vom 6. April 2016, beim Gerichtshof eingegangen am 14. April 2016, in dem Verfahren auf Betreiben des

Ministerio Fiscal

erlässt

DER GERICHTSHOF (Große Kammer)

unter Mitwirkung des Präsidenten K. Lenaerts, des Vizepräsidenten A. Tizzano, der Kammerpräsidentin R. Silva de Lapuerta, der Kammerpräsidenten T. von Danwitz (Berichterstatter), J. L. da Cruz Vilaça, C. G. Fernlund und C. Vajda, der Richter E. Juhász und A. Borg Barthet, der Richterin C. Toader, der Richter M. Safjan und D. Šváby, der Richterin M. Berger sowie der Richter E. Jarašiūnas und E. Regan,

Generalanwalt: H. Saugmandsgaard Øe,

Kanzler: L. Carrasco Marco, Verwaltungsrätin,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 29. Januar 2018,

unter Berücksichtigung der Erklärungen

– des Ministerio Fiscal, vertreten durch E. Tejada de la Fuente,

– der spanischen Regierung, vertreten durch M. Sampol Pucurull als Bevollmächtigten,

– der tschechischen Regierung, vertreten durch M. Smolek, J. Vláčil und A. Brabcová als Bevollmächtigte,

– der dänischen Regierung, vertreten durch J. Nymann-Lindegren und M. Wolff als Bevollmächtigte,

* Verfahrenssprache: Spanisch.

– der estnischen Regierung, vertreten durch N. Grünberg als Bevollmächtigte,

– von Irland, vertreten durch M. Browne, L. Williams, E. Creedon und A. Joyce als Bevollmächtigte im Beistand von E. Gibson, BL,

– der französischen Regierung, vertreten durch D. Colas, E. de Moustier und E. Armoet als Bevollmächtigte,

– der lettischen Regierung, vertreten durch I. Kucina und J. Davidoviča als Bevollmächtigte,

– der ungarischen Regierung, vertreten durch M. Fehér und G. Koós als Bevollmächtigte,

– der österreichischen Regierung, vertreten durch C. Pesendorfer als Bevollmächtigte,

– der polnischen Regierung, vertreten durch B. Majczyna, D. Lutostańska und J. Sawicka als Bevollmächtigte,

– der Regierung des Vereinigten Königreichs, vertreten durch S. Brandon und C. Brodie als Bevollmächtigte im Beistand von M. C. Knight, Barrister, und G. Facenna, QC,

– der Europäischen Kommission, vertreten durch I. Martínez del Peral, P. Costa de Oliveira, R. Troosters und D. Nardi als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 3. Mai 2018

folgendes

Urteil

1 Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 15 Abs. 1 der 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 (im Folgenden: Richtlinie 2002/58) im Licht der Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).

2 Dieses Ersuchen ergeht im Rahmen eines Rechtsmittels des Ministerio Fiscal (Staatsanwaltschaft, Spanien) gegen die Entscheidung des Juzgado de Instrucción nº 3 de Tarragona (Ermittlungsrichter Nr. 3 von Tarragona, im Folgenden: Ermittlungsrichter), mit der es abgelehnt wurde, der Kriminalpolizei den Zugang zu von Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten zu erlauben.

Rechtlicher Rahmen

Unionsrecht

Richtlinie 95/46

3 Nach Art. 2 Buchst. b der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31) bezeichnet der Ausdruck „Verarbeitung personenbezogener Daten“ im Sinne dieser Richtlinie „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten“.

4 Art. 3 („Anwendungsbereich“) dieser Richtlinie sieht vor:

„(1) Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

(2) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,

– die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;

– die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.“

Richtlinie 2002/58

5 In den Erwägungsgründen 2, 11, 15 und 21 der Richtlinie 2002/58 heißt es:

„(2) Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die [Charta] anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 [der] Charta niedergelegten Rechte uneingeschränkt geachtet werden.

…

(11) Wie die Richtlinie [95/46] gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das Gemeinschaftsrecht fallen. Deshalb hat sie keine Auswirkungen auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten, Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die

Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein sowie angemessenen Garantien gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten entsprechen.

…

(15) Eine Nachricht kann alle Informationen über Namen, Nummern oder Adressen einschließen, die der Absender einer Nachricht oder der Nutzer einer Verbindung für die Zwecke der Übermittlung der Nachricht bereitstellt. Der Begriff ‚Verkehrsdaten' kann alle Formen einschließen, in die diese Informationen durch das Netz, über das die Nachricht übertragen wird, für die Zwecke der Übermittlung umgewandelt werden. …

…

(21) Es sollten Maßnahmen getroffen werden, um den unerlaubten Zugang zu Nachrichten – und zwar sowohl zu ihrem Inhalt als auch zu mit ihnen verbundenen Daten – zu verhindern und so die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen elektronischen Kommunikationsdiensten erfolgenden Nachrichtenübertragung zu schützen. Nach dem Recht einiger Mitgliedstaaten ist nur der absichtliche unberechtigte Zugriff auf die Kommunikation untersagt."

6 Art. 1 („Geltungsbereich und Zielsetzung") der Richtlinie 2002/58 bestimmt:

„(1) Diese Richtlinie sieht die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie [95/46] im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich."

7 In Art. 2 („Begriffsbestimmungen") der Richtlinie 2002/58 heißt es:

„Sofern nicht anders angegeben, gelten die Begriffsbestimmungen der Richtlinie [95/46] und der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste („Rahmenrichtlinie") [ABl. 2002, L 108, S. 33] auch für diese Richtlinie.

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

…

b) ‚Verkehrsdaten' Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

c) ‚Standortdaten' Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben;

d) ‚Nachricht' jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein elektronisches Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

…"

8 Art. 3 („Betroffene Dienste") der Richtlinie 2002/58 sieht vor:

„Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen."

9 In Art. 5 („Vertraulichkeit der Kommunikation") der Richtlinie 2002/58 heißt es:

„(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. …

…

(3) Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie [95/46] u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. …"

10 Art. 6 („Verkehrsdaten") der Richtlinie 2002/58 bestimmt:

„(1) Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.

(2) Verkehrsdaten, die zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, dürfen verarbeitet werden. Diese Verarbeitung ist nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann.

…“

11 Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) der Richtlinie sieht in Abs. 1 vor:

„(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie [95/46] für die nationale Sicherheit, (d. h. die Sicherheit des Staates), 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. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.“

Spanisches Recht

Gesetz 25/2007

12 Art. 1 der Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (Gesetz 25/2007 über die Speicherung von Daten betreffend die elektronische Kommunikation und öffentliche Kommunikationsnetzwerke) vom 18. Oktober 2007 (BOE Nr. 251 vom 19. Oktober 2007, S. 42517) bestimmt:

„1. Zweck dieses Gesetzes ist die Regelung der Pflicht der Betreiber, die im Rahmen elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugten oder verarbeiteten Daten zu speichern, sowie der Pflicht, solche Daten den befugten Bediensteten zu übermitteln, wenn sie mittels der entsprechenden gerichtlichen Erlaubnis zu Zwecken der Aufdeckung, Ermittlung und Verfolgung schwerer Straftaten im Sinne des Strafgesetzbuchs oder der Sonderstrafgesetze angefordert werden.

2. Dieses Gesetz gilt für Verkehrs- und Standortdaten sowohl von juristischen als auch von natürlichen Personen sowie für alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind.

…“

Strafgesetzbuch

13 Art. 13 Abs. 1 der Ley Orgánica 10/1995 del Código Penal (Strafgesetzbuch) vom 23. November 1995 (BOE Nr. 281 vom 24. November 1995, S. 33987) lautet:

„Schwere Straftaten sind Straftaten, die nach dem Gesetz mit schwerer Strafe bedroht sind.“

14 Art. 33 dieses Gesetzes sieht vor:

„1. Je nach ihrer Art und Dauer werden Strafen in schwere, weniger schwere und leichte eingeteilt.

2. Zu den schweren Strafen gehören:

a) lebenslange Freiheitsstrafe mit der Möglichkeit der vorzeitigen Haftentlassung;

b) Freiheitsstrafe von mehr als fünf Jahren;

…“

Strafprozessordnung

15 Die Ley de Enjuiciamiento Criminal (Strafprozessordnung) wurde nach dem entscheidungserheblichen Zeitraum durch die Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (Organgesetz 13/2015 zur Änderung der Strafprozessordnung durch Stärkung der Verfahrensgarantien und Regelung der technologischen Untersuchungsmaßnahmen) vom 5. Oktober 2015 (BOE Nr. 239 vom 6. Oktober 2015, S. 90192) geändert.

16 Dieses Gesetz trat am 6. Dezember 2015 in Kraft. Mit ihm wurde der Bereich des Zugangs zu den von Betreibern elektronischer Kommunikationsdienste im Zusammenhang mit telefonischen und telematischen Kommunikationsvorgängen gespeicherten Daten in die Strafprozessordnung aufgenommen.

17 Art. 579 Abs. 1 der Strafprozessordnung in der Fassung des Organgesetzes 13/2015 sieht vor:

„1. Das Gericht kann das Abfangen privater postalischer und telegrafischer Korrespondenz einschließlich der Korrespondenz per Telefax, ‚Burofax‘ und internationaler Postanweisung, die der Verdächtige versendet oder erhält, sowie das Öffnen und Prüfen dieser Korrespondenz erlauben, wenn Indizien Anlass zu der Annahme geben, dass dies zur Auffindung oder zum Nachweis einer Tatsache oder eines relevanten Faktors führen wird, sofern die Ermittlung eine der folgenden Straftaten zum Gegenstand hat:

1) vorsätzliche Straftaten, die im Höchstmaß mit Freiheitsstrafe von mindestens drei Jahren bedroht sind,

2) Straftaten, die im Rahmen einer kriminellen Vereinigung oder Organisation begangen werden, und

3) terroristische Straftaten.

…“

18 Art. 588 ter j dieses Gesetzbuchs sieht vor:

„1. Elektronische Daten, die von den Dienstleistungserbringern oder von Personen, die die Kommunikation ermöglichen, im Einklang mit den Rechtsvorschriften über die Speicherung von Daten betreffend die elektronische Kommunikation oder aus eigener Initiative aus wirtschaftlichen oder anderen Gründen gespeichert werden und die mit Kommunikationsvorgängen verbunden sind, dürfen zur Heranziehung in einem Verfahren nur mit gerichtlicher Erlaubnis übermittelt werden.

2. Erweist sich die Kenntnis dieser Daten als für die Ermittlung unerlässlich, ist beim zuständigen Richter die Erlaubnis zur Einholung der in den automatisierten Archiven der Dienstleistungserbringer befindlichen Informationen, einschließlich der Kreuz- oder intelligenten Abfrage von Daten, zu beantragen, wobei die Art der Daten, deren Kenntnis erforderlich ist, und die ihre Übermittlung rechtfertigenden Gründe anzugeben sind."

Ausgangsverfahren und Vorlagefragen

19 Herr Hernández Sierra erstattete bei der Polizei Anzeige wegen des Raubs seiner Brieftasche und seines Mobiltelefons, der sich am 16. Februar 2015 zugetragen habe und bei dem er verletzt worden sei.

20 Mit Schreiben vom 27. Februar 2015 beantragte die Kriminalpolizei beim Ermittlungsrichter, verschiedenen Betreibern elektronischer Kommunikationsdienste aufzugeben, die vom 16. bis zum 27. Februar 2015 mit der internationalen Mobilfunkgerätekennung (im Folgenden: IMEI [International Mobile Equipment Identity]) des gestohlenen Mobiltelefons aktivierten Telefonnummern sowie die personenbezogenen Daten über die Identität der Inhaber oder Nutzer der den mit diesem Code aktivierten Telefonnummern entsprechenden SIM-Karten, wie ihren Namen, ihren Vornamen und gegebenenfalls ihre Adresse, zu übermitteln.

21 Mit Beschluss vom 5. Mai 2015 wies der Ermittlungsrichter diesen Antrag zurück. Er stellte zum einen fest, dass die beantragte Maßnahme zur Identifizierung der Straftäter nicht geeignet sei. Zum anderen lehnte er es ab, dem Antrag stattzugeben, weil das Gesetz 25/2007 die Übermittlung der von den Betreibern elektronischer Kommunikationsdienste gespeicherten Daten auf schwere Straftaten beschränke. Nach dem Strafgesetzbuch seien schwere Straftaten mit Freiheitsstrafen von mehr als fünf Jahren bedroht, während der Sachverhalt des Ausgangsverfahrens keine solche Straftat darzustellen scheine.

22 Die Staatsanwaltschaft legte gegen diesen Beschluss bei der Audiencia Provincial de Tarragona (Regionalgericht Tarragona, Spanien) Berufung ein und machte geltend, dass die Übermittlung der in Rede stehenden Daten aufgrund der Art des Sachverhalts und eines in einem ähnlichen Fall ergangenen Urteils des Tribunal Supremo (Oberster Gerichtshof, Spanien) vom 26. Juli 2010 hätte gewährt werden müssen.

23 Das vorlegende Gericht führt aus, dass der spanische Gesetzgeber nach jenem Beschluss die Strafprozessordnung durch Erlass des Organgesetzes 13/2015 geändert habe. Mit diesem Gesetz, das für den Ausgang des Verfahrens im Ausgangsrechtsstreit relevant sei, seien zwei neue alternative Kriterien für die Bestimmung der Schwere einer Straftat eingeführt worden. Zum einen handele es sich um ein materielles Kriterium, das an Verhaltensweisen von besonderer und erheblicher kriminogener Relevanz anknüpfe, die Individual- und Kollektivrechtsgüter besonders schädigten. Zum anderen habe der nationale Gesetzgeber ein normativ-formales Kriterium herangezogen, dem die für die betreffende Straftat vorgesehene Strafe zugrunde liege. Die Mindeststrafe von drei Jahren Freiheitsentzug, den die Strafprozessordnung nunmehr vorsehe, erfasse allerdings die große Mehrheit der Straftaten. Zudem könne das staatliche Interesse an der Bekämpfung strafbaren Verhaltens keinen unverhältnismäßigen Eingriff in die in der Charta verankerten Grundrechte rechtfertigen.

24 Insoweit stellen nach Ansicht dieses Gerichts die Richtlinien 95/46 und 2002/58 im Ausgangsverfahren den Bezug zur Charta her. Die im Ausgangsverfahren in Rede stehende nationale Regelung falle daher nach Art. 51 Abs. 1 der Charta ungeachtet der Ungültigerklärung der 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) durch das Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), in den Anwendungsbereich der Charta.

25 Der Gerichtshof habe in diesem Urteil anerkannt, dass die Vorratsspeicherung und Übermittlung von Verkehrsdaten besonders schwere Eingriffe in die durch die Art. 7 und 8 der Charta gewährleisteten Rechte darstellten, und die Kriterien für die Beurteilung der Beachtung des Verhältnismäßigkeitsgrundsatzes festgestellt, zu denen die Schwere der Straftaten gehöre, die die Vorratsspeicherung dieser Daten und den Zugang dazu zu Ermittlungszwecken rechtfertigten.

26 Unter diesen Umständen hat die Audiencia Provincial de Tarragona (Regionalgericht Tarragona) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Kann die hinreichende Schwere der Straftaten als Kriterium, das einen Eingriff in die Grundrechte rechtfertigt, die in den Art. 7 und 8 der Charta anerkannt werden, allein anhand der Strafe ermittelt werden, die wegen der untersuchten Straftat verhängt werden kann, oder müssen daneben bei dem deliktischen Verhalten bestimmte Grade der Schädlichkeit für Individual- und/oder Kollektivrechtsgüter festgestellt werden?

2. Falls die Ermittlung der Schwere der Straftat allein anhand der in Betracht kommenden Strafe mit den Verfassungsgrundsätzen der Union, die der Gerichtshof in seinem Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), als Standards für die strikte Kontrolle der Richtlinie 2002/58 herangezogen hat, vereinbar ist, wie hoch muss dann die Mindeststrafe sein? Wäre eine allgemeine Grenze von drei Jahren Freiheitsentzug zulässig?

Verfahren vor dem Gerichtshof

27 Mit Entscheidung des Präsidenten des Gerichtshofs vom 23. Mai 2016 ist das Verfahren vor dem Gerichtshof bis zur Verkündung des Urteils in den verbundenen Rechtssachen Tele2 Sverige und Watson u. a., C-203/15 und C-698/15 (Urteil vom 21. Dezember 2016, EU:C:2016:970, im Folgenden: Urteil Tele2 Sverige und Watson u. a.), ausgesetzt worden. Nach der Verkündung dieses Urteils wurde das vorlegende Gericht gefragt, ob es sein Vorabentscheidungsersuchen aufrechterhalten oder zurückziehen wolle. Das vorlegende Gericht hat darauf mit Schreiben vom 30. Januar 2017, das am 14. Februar 2017 beim Gerichtshof eingegangen ist, geantwortet, dass dieses Urteil es ihm nicht ermögliche, die im Ausgangsverfahren in Rede stehende nationale Regelung mit hinreichender Sicherheit unionsrechtlich zu beurteilen. Das Verfahren vor dem Gerichtshof ist daher am 16. Februar 2017 wieder aufgenommen worden.

Zu den Vorlagefragen

28 Die spanische Regierung wendet zum einen ein, dass der Gerichtshof für die Beantwortung des Vorabentscheidungsersuchens unzuständig sei, und zum anderen, dass dieses Ersuchen unzulässig sei.

Zur Zuständigkeit des Gerichtshofs

29 Die spanische Regierung hat in ihren beim Gerichtshof eingereichten schriftlichen Erklärungen die Auffassung vertreten – der sich die Regierung des Vereinigten Königreichs in der mündlichen Verhandlung angeschlossen hat –, dass der Gerichtshof für die Beantwortung des Vorabentscheidungsersuchens unzuständig sei, weil die Ausgangsrechtssache nach Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 und Art. 1 Abs. 3 der Richtlinie 2002/58 vom Geltungsbereich dieser beiden Richtlinien ausgenommen sei. Diese Rechtssache falle daher nicht in den Geltungsbereich des Unionsrechts, so dass die Charta gemäß ihrem Art. 51 Abs. 1 nicht anwendbar sei.

30 Der Gerichtshof habe zwar im Urteil Tele2 Sverige und Watson u. a. entschieden, dass eine Rechtsvorschrift, die den Zugang der nationalen Behörden zu den von den Betreibern elektronischer Kommunikationsdienste gespeicherten Daten regele, in den Geltungsbereich der Richtlinie 2002/58 falle. Im vorliegenden Fall handele es sich jedoch um einen kraft gerichtlicher Entscheidung im Rahmen eines strafrechtlichen Ermittlungsverfahrens ergehenden Antrag einer öffentlichen Stelle auf Zugang zu von den Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten. Die spanische Regierung schließt daraus, dass dieser Zugangsantrag im Rahmen der Ausübung des *ius puniendi* durch die nationalen Behörden gestellt werde, so dass er eine Tätigkeit des Staates im strafrechtlichen Bereich darstelle, die unter die Ausnahmeregelung in Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 und Art. 1 Abs. 3 der Richtlinie 2002/58 falle.

31 Zur Beurteilung dieser Einrede der Unzuständigkeit ist darauf hinzuweisen, dass Art. 1 der Richtlinie 2002/58 in Abs. 1 vorsieht, dass diese Richtlinie der Harmonisierung der nationalen Vorschriften dient, die erforderlich sind, um u. a. einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation zu gewährleisten. Nach ihrem Art. 1 Abs. 2 stellt diese Richtlinie eine Detaillierung und Ergänzung der Richtlinie 95/46 im Hinblick auf die in dem genannten Abs. 1 angeführten Zwecke dar.

32 Art. 1 Abs. 3 der Richtlinie 2002/58 schließt von ihrem Geltungsbereich die „Tätigkeiten des Staates“ in den dort vorgesehenen Bereichen aus, zu denen die Tätigkeiten des Staates im strafrechtlichen Bereich sowie die Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt, gehören (Urteil Tele2 Sverige und Watson u. a., Rn. 69 und die dort angeführte Rechtsprechung). Die dort beispielhaft aufgeführten Tätigkeiten sind allesamt spezifische Tätigkeiten der Staaten oder staatlicher Stellen, die nichts mit den Tätigkeitsbereichen von Privatpersonen zu tun haben (vgl. entsprechend zu Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 Urteil vom 10. Juli 2018, Jehovan Todistajat, C-25/17, EU:C:2018:551, Rn. 38 und die dort angeführte Rechtsprechung).

33 Nach Art. 3 der Richtlinie 2002/58 gilt diese für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen (im Folgenden: elektronische Kommunikationsdienste). Folglich ist davon auszugehen, dass diese Richtlinie die Tätigkeiten der Betreiber solcher Dienste regelt (Urteil Tele2 Sverige und Watson u. a., Rn. 70).

34 Zu Art. 15 Abs. 1 der Richtlinie 2002/58 hat der Gerichtshof bereits entschieden, dass die Rechtsvorschriften, um die es in dieser Vorschrift geht, in den Geltungsbereich dieser Richtlinie fallen, auch wenn sie sich auf spezifische Tätigkeiten der Staaten oder der staatlichen Stellen beziehen, die mit den Tätigkeitsbereichen von Einzelpersonen nichts zu tun haben, und die Zweckbestimmungen, denen diese Rechtsvorschriften entsprechen müssen, sich im Wesentlichen mit den Zielen, die mit den in Art. 1 Abs. 3 der Richtlinie 2002/58 genannten Tätigkeiten verfolgt werden, decken. Art. 15 Abs. 1 dieser Richtlinie setzt nämlich zwangsläufig voraus, dass die dort genannten nationalen Vorschriften in den Geltungsbereich der Richtlinie fallen, da diese Richtlinie die Mitgliedstaaten zum Erlass solcher Vorschriften ausdrücklich nur dann ermächtigt, wenn die darin vorgesehenen Voraussetzungen eingehalten werden. Außerdem regeln die in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Rechtsvorschriften – zu den in dieser Bestimmung genannten Zwecken – die Tätigkeit der Betreiber elektronischer Kommunikationsdienste (vgl. in diesem Sinne Urteil Tele2 Sverige und Watson u. a., Rn. 72 bis 74).

35 Der Gerichtshof ist zu dem Schluss gelangt, dass der genannte Art. 15 Abs. 1 in Verbindung mit Art. 3 der Richtlinie 2002/58 dahin auszulegen ist, dass in den Geltungsbereich dieser Richtlinie nicht nur eine Rechtsvorschrift fällt, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, die

Verkehrs- und Standortdaten zu speichern, sondern auch eine Rechtsvorschrift, die den Zugang der nationalen Behörden zu den von diesen Betreibern gespeicherten Daten betrifft (vgl. in diesem Sinne Urteil Tele2 Sverige und Watson u. a., Rn. 75 und 76).

36 Der durch Art. 5 Abs. 1 der Richtlinie 2002/58 garantierte Schutz der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Verkehrsdaten gilt nämlich für Maßnahmen sämtlicher anderer Personen als der Nutzer, unabhängig davon, ob es sich um private Personen oder Einrichtungen oder um staatliche Einrichtungen handelt. Wie ihr 21. Erwägungsgrund bestätigt, soll die Richtlinie 2002/58 jeden unerlaubten Zugang zu Nachrichten einschließlich zu „mit ihnen verbundenen Daten“ verhindern, um die Vertraulichkeit elektronischer Kommunikationen zu schützen (Urteil Tele2 Sverige und Watson u. a., Rn. 77).

37 Ferner ist anzumerken, dass Rechtsvorschriften, die den Betreibern elektronischer Kommunikationsdienste vorschreiben, personenbezogene Daten zu speichern oder den zuständigen nationalen Behörden den Zugang zu diesen Daten zu gewähren, zwangsläufig die Verarbeitung dieser Daten durch die Betreiber zur Folge haben (vgl. in diesem Sinne Urteil Tele2 Sverige und Watson u. a., Rn. 75 und 78). Da solche Vorschriften die Tätigkeiten dieser Betreiber regeln, können sie somit nicht den in Art. 1 Abs. 3 der Richtlinie 2002/58 genannten spezifischen Tätigkeiten der Staaten gleichgestellt werden.

38 Wie aus der Vorlageentscheidung hervorgeht, wurde im vorliegenden Fall der im Ausgangsverfahren in Rede stehende Antrag, mit dem die Kriminalpolizei um eine gerichtliche Erlaubnis ersucht, um Zugang zu von Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten zu erhalten, auf das Gesetz 25/2007 – in Verbindung mit der Strafprozessordnung in seiner im entscheidungserheblichen Zeitraum geltenden Fassung – gestützt, das den Zugang öffentlicher Stellen zu solchen Daten regelt. Diese Regelung räumt der Kriminalpolizei im Fall einer auf ihrer Grundlage erteilten gerichtlichen Erlaubnis das Recht ein, von den Betreibern elektronischer Kommunikationsdienste zu verlangen, ihr personenbezogene Daten bereitzustellen und damit angesichts der in Art. 2 Buchst. b der Richtlinie 95/46 enthaltenen Begriffsbestimmung, die nach Art. 2 Abs. 1 der Richtlinie 2002/58 in deren Rahmen anwendbar ist, eine „Verarbeitung“ solcher Daten im Sinne dieser beiden Richtlinien vorzunehmen. Diese Regelung betrifft daher die Tätigkeiten der Betreiber elektronischer Kommunikationsdienste und fällt somit in den Geltungsbereich der Richtlinie 2002/58.

39 Unter diesen Umständen kann der von der spanischen Regierung vorgebrachte Umstand, dass dieser Zugangsantrag im Rahmen eines strafrechtlichen Ermittlungsverfahrens gestellt wurde, nicht dazu führen, dass die Richtlinie 2002/58 nach ihrem Art. 1 Abs. 3 auf die Ausgangsrechtssache keine Anwendung findet.

40 Insoweit ist ebenfalls unerheblich, dass, wie aus der schriftlichen Antwort der spanischen Regierung auf eine Frage des Gerichtshofs hervorgeht und wie sowohl diese Regierung als auch die Staatsanwaltschaft in der mündlichen Verhandlung bestätigt haben, der im Ausgangsverfahren in Rede stehende Zugangsantrag den Zugang nur zu den Telefonnummern, die den mit der IMEI des gestohlenen Mobiltelefons aktivierten SIM-Karten entsprechen, und zu den Daten über die Identität der Inhaber dieser Karten wie deren Name, Vorname und gegebenenfalls Adresse ermöglichen soll, nicht jedoch zu den Daten über die mittels dieser SIM-Karten erfolgte Kommunikation und den Standortdaten des gestohlenen Mobiltelefons.

41 Wie der Generalanwalt in Nr. 54 seiner Schlussanträge ausgeführt hat, regelt die Richtlinie 2002/58 nämlich nach ihrem Art. 1 Abs. 1 und ihrem Art. 3 jegliche Verarbeitung personenbezogener Daten im Rahmen der Erbringung von elektronischen Kommunikationsdiensten. Ferner erfasst der Begriff „Verkehrsdaten“ nach Art. 2 Abs. 2 Buchst. b dieser Richtlinie „Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden“.

42 Was diesen letzten Punkt, insbesondere Daten über die Identität der Inhaber von SIM-Karten, betrifft, ergibt sich aus dem 15. Erwägungsgrund der Richtlinie 2002/58, dass Verkehrsdaten u. a. den Namen und die Adresse des Absenders einer Nachricht oder des Nutzers einer Verbindung für die Zwecke der Übermittlung der Nachricht einschließen können. Die Daten über die Identität der Inhaber von SIM-Karten können sich ferner als für die Fakturierung der erbrachten elektronischen Kommunikationsdienste erforderlich erweisen und gehören daher zu den Verkehrsdaten im Sinne der Definition in Art. 2 Abs. 2 Buchst. b dieser Richtlinie. Diese Daten fallen folglich in den Geltungsbereich der Richtlinie 2002/58.

43 Der Gerichtshof ist daher für die Beantwortung der Frage des vorlegenden Gerichts zuständig.

Zur Zulässigkeit

44 Die spanische Regierung hält das Vorabentscheidungsersuchen für unzulässig, da darin die unionsrechtlichen Vorschriften nicht eindeutig bezeichnet seien, zu denen sich der Gerichtshof äußern solle. Außerdem beziehe sich der im Ausgangsverfahren in Rede stehende Antrag der Kriminalpolizei nicht auf die Überwachung der Kommunikation, die mittels der mit der IMEI des gestohlenen Mobiltelefons aktivierten SIM-Karten erfolgt sei, sondern auf die Herstellung einer Verbindung zwischen diesen Karten und ihren Inhabern, so dass die Vertraulichkeit der Kommunikation nicht beeinträchtigt werde. Der in den Vorlagefragen genannte Art. 7 der Charta sei daher im Zusammenhang mit der vorliegenden Rechtssache irrelevant.

45 Nach ständiger Rechtsprechung des Gerichtshofs ist es allein Sache des mit dem Rechtsstreit befassten nationalen Gerichts, in dessen Verantwortungsbereich die zu erlassende gerichtliche Entscheidung fällt, im Hinblick auf die Besonderheiten der Rechtssache sowohl die Erforderlichkeit einer Vorabentscheidung zum Erlass seines Urteils als auch die Erheblichkeit der dem Gerichtshof vorgelegten Fragen zu beurteilen. Daher ist der Gerichtshof grundsätzlich gehalten, über die ihm vorgelegten Fragen zu befinden, wenn sie die Auslegung des Unionsrechts betreffen. Der Gerichtshof kann die Beantwortung einer Vorlagefrage eines nationalen Gerichts nur ablehnen, wenn die erbetene Auslegung des Unionsrechts offensichtlich in keinem Zusammenhang mit der Realität oder dem Gegenstand des Ausgangsrechtsstreits steht, wenn das Problem hypothetischer Natur ist oder wenn der Gerichtshof nicht über die tatsächlichen und rechtlichen Angaben verfügt, die für eine zweckdienliche Beantwortung der ihm vorgelegten Fragen erforderlich sind (Urteil vom 10. Juli 2018, Jehovan Todistajat, C-25/17, EU:C:2018:551, Rn. 31 und die dort angeführte Rechtsprechung).

46 Im vorliegenden Fall enthält die Vorlageentscheidung die tatsächlichen und rechtlichen Angaben, die sowohl für die Bestimmung der Vorschriften des Unionsrechts, auf die sich die Vorlagefragen beziehen, als auch für das Verständnis der Tragweite dieser Fragen genügen. Insbesondere geht aus der Vorlageentscheidung hervor, dass die Vorlagefragen dem vorlegenden Gericht die Beurteilung der Frage ermöglichen sollen, ob und inwieweit mit der nationalen Regelung, auf die der im Ausgangsverfahren in Rede stehende Antrag der Kriminalpolizei gestützt wurde, ein Zweck verfolgt wird, der einen Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte rechtfertigen kann. Den Angaben des vorlegenden Gerichts zufolge fällt diese nationale Regelung in den Geltungsbereich der Richtlinie 2002/58, so dass die Charta in der Ausgangsrechtssache anwendbar ist. Die Vorlagefragen weisen daher einen unmittelbaren Bezug zum Gegenstand des Ausgangsverfahrens auf und können somit nicht als hypothetisch angesehen werden.

47 Nach alledem sind die Vorlagefragen zulässig.

Zur Beantwortung der Fragen

48 Mit seinen beiden Fragen, die zusammen zu prüfen sind, möchte das vorlegende Gericht wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 der Charta dahin auszulegen ist, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta verankerte Grundreche darstellt, der so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste, und nach welchen Kriterien bejahendenfalls die Schwere der in Rede stehenden Straftat zu beurteilen ist.

49 Insoweit geht, wie der Generalanwalt in Nr. 38 seiner Schlussanträge ausgeführt hat, aus dem Vorabentscheidungsersuchen hervor, dass mit diesem nicht geklärt werden soll, ob die im Ausgangsverfahren in Rede stehenden personenbezogenen Daten von den Betreibern elektronischer Kommunikationsdienste unter Beachtung der in Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 der Charta vorgesehenen Voraussetzungen gespeichert wurden. Das Ersuchen bezieht sich, wie sich aus Rn. 46 des vorliegenden Urteils ergibt, nur auf die Frage, ob und inwieweit der Zweck der im Ausgangsverfahren in Rede stehenden Regelung geeignet ist, den Zugang öffentlicher Stellen wie der Kriminalpolizei zu solchen Daten zu rechtfertigen, ohne dass die übrigen Zugangsvoraussetzungen nach diesem Art. 15 Abs. 1 Gegenstand dieses Ersuchens wären.

50 Das vorlegende Gericht möchte insbesondere wissen, nach welchen Gesichtspunkten zu beurteilen ist, ob die Straftaten, bezüglich deren den Polizeibehörden zu Ermittlungszwecken der Zugang zu personenbezogenen Daten erlaubt wird, die die Betreiber elektronischer Kommunikationsdienste gespeichert haben, hinreichend schwer sind, um den mit einem solchen Zugang verbundenen Eingriff in die in den Art. 7 und 8 der Charta gewährleisteten Grundrechte, wie sie vom Gerichtshof in seinen Urteilen vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), und Tele2 Sverige und Watson u. a., ausgelegt worden sind, zu rechtfertigen.

51 Was das Vorliegen eines Eingriffs in diese Grundrechte betrifft, stellt, wie der Generalanwalt in den Nrn. 76 und 77 seiner Schlussanträge ausgeführt hat, der Zugang der öffentlichen Stellen zu solchen Daten einen Eingriff in das in Art. 7 der Charta verankerte Grundrecht auf Achtung des Privatlebens dar, auch wenn keine Umstände vorliegen, aufgrund deren dieser Eingriff als „schwer“ eingestuft werden kann, und ohne dass es darauf ankommt, ob die betroffenen Informationen über das Privatleben als sensibel anzusehen sind oder die Betroffenen durch diesen Eingriff irgendwelche Nachteile erlitten haben. Zudem stellt ein solcher Zugang einen Eingriff in das in Art. 8 der Charta garantierte Grundrecht auf Schutz personenbezogener Daten dar, da es sich dabei um eine Verarbeitung personenbezogener Daten handelt (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 124 und 126 sowie die dort angeführte Rechtsprechung).

52 Hinsichtlich der Zwecke, die eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende – die den Zugang öffentlicher Stellen zu von Betreibern elektronischer Kommunikationsdienste gespeicherten Daten betrifft und damit vom Grundsatz der Vertraulichkeit elektronischer Kommunikationen abweicht – rechtfertigen können, ist darauf hinzuweisen, dass die Aufzählung der in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 genannten Zwecke abschließend ist, so dass dieser Zugang tatsächlich strikt einem dieser Zwecke dienen muss (vgl. in diesem Sinne Urteil Tele2 Sverige und Watson u. a., Rn. 90 und 115).

53 Was den Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten anbelangt, ist aber festzustellen, dass dieser nach dem Wortlaut von Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 nicht auf die Bekämpfung schwerer Straftaten beschränkt ist, sondern „Straftaten“ im Allgemeinen betrifft.

54 Insoweit hat der Gerichtshof zwar entschieden, dass im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur die Bekämpfung der schweren Kriminalität einen Zugang öffentlicher Stellen zu von den Betreibern von Kommunikationsdiensten gespeicherten personenbezogenen Daten rechtfertigen kann, aus deren Gesamtheit genaue Schlüsse auf das Privatleben der von diesen Daten betroffenen Personen gezogen werden können (vgl. in diesem Sinne Urteil Tele2 Sverige und Watson u. a., Rn. 99).

55 Der Gerichtshof hat diese Auslegung jedoch damit begründet, dass der mit einer solchen Zugangsregelung verfolgte Zweck im Verhältnis zur Schwere des damit einhergehenden Eingriffs in die betreffenden Grundrechte stehen muss (vgl. in diesem Sinne Urteil Tele2 Sverige und Watson u. a., Rn. 115).

56 Nach dem Grundsatz der Verhältnismäßigkeit kann ein schwerer Eingriff im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nämlich nur durch einen Zweck der Bekämpfung einer ebenfalls als „schwer“ einzustufenden Kriminalität gerechtfertigt sein.

57 Ist dagegen der mit einem solchen Zugang verbundene Eingriff nicht schwer, kann dieser Zugang durch einen Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von „Straftaten“ im Allgemeinen gerechtfertigt sein.

58 Es ist daher zunächst zu prüfen, ob nach den Umständen des vorliegenden Falles der Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte, der mit einem Zugang der Kriminalpolizei zu den im Ausgangsverfahren in Rede stehenden Daten einhergeht, als „schwer“ anzusehen ist.

59 Insoweit ist festzustellen, dass der im Ausgangsverfahren in Rede stehende Antrag, mit dem die Kriminalpolizei für die Zwecke strafrechtlicher Ermittlungen um gerichtliche Erlaubnis zum Zugang zu von den Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten ersucht, ausschließlich darauf abzielt, die Identität der Inhaber von SIM-Karten festzustellen, die in einem Zeitraum von zwölf Tagen mit der IMEI des gestohlenen Mobiltelefons aktiviert wurden. Wie in Rn. 40 des vorliegenden Urteils ausgeführt, bezieht sich dieser Antrag nur auf den Zugang zu den diesen SIM-Karten entsprechenden Telefonnummern sowie zu den Daten bezüglich der Identität der Karteninhaber wie deren Name, Vorname und gegebenenfalls Adresse. Dagegen beziehen sich diese Daten, wie sowohl die spanische Regierung als auch die Staatsanwaltschaft in der mündlichen Verhandlung bestätigt haben, weder auf die mittels des gestohlenen Mobiltelefons erfolgte Kommunikation noch auf dessen Ortung.

60 Daher kann mit den Daten, auf die sich der im Ausgangsverfahren in Rede stehende Zugangsantrag bezieht, offenbar nur eine Verbindung zwischen der SIM-Karte oder den SIM-Karten, die mit dem gestohlenen Mobiltelefon aktiviert wurden, und der Identität der Inhaber dieser SIM-Karten während eines bestimmten Zeitraums hergestellt werden. Ohne einen Abgleich mit den Daten bezüglich der mittels dieser SIM-Karten erfolgten Kommunikation und den Standortdaten lassen sich diesen Daten weder das Datum, die Uhrzeit, die Dauer und die Adressaten der mittels der betreffenden SIM-Karte bzw. der betreffenden SIM-Karten erfolgten Kommunikation entnehmen noch die Orte, an denen diese Kommunikation erfolgte, oder die Häufigkeit dieser Kommunikation mit bestimmten Personen während eines bestimmten Zeitraums. Aus diesen Daten lassen sich daher keine genauen Schlüsse auf das Privatleben der Personen ziehen, deren Daten betroffen sind.

61 Unter diesen Umständen kann der Zugang nur zu den Daten, auf die sich der im Ausgangsverfahren in Rede stehende Antrag bezieht, nicht als „schwerer“ Eingriff in die Grundrechte der Personen eingestuft werden, deren Daten betroffen sind.

62 Wie sich aus den Rn. 53 bis 57 des vorliegenden Urteils ergibt, kann der Eingriff, den ein Zugang zu solchen Daten mit sich bringen würde, somit durch den in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 genannten Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von „Straftaten" im Allgemeinen gerechtfertigt sein, ohne dass es erforderlich wäre, dass diese Straftaten als „schwer" einzustufen sind.

63 Nach alledem ist auf die Vorlagefragen zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 der Charta dahin auszulegen ist, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta verankerte Grundreche darstellt, der nicht so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste.

Kosten

64 Für die Beteiligten des Ausgangsverfahrens ist das Verfahren Teil des beim vorlegenden Gericht anhängigen Verfahrens; die Kostenentscheidung ist daher Sache dieses Gerichts. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

Aus diesen Gründen hat der Gerichtshof (Große Kammer) für Recht erkannt:

Art. 15 Abs. 1 der 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) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7 und 8 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta der Grundrechte verankerte Grundreche darstellt, der nicht so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste.

Unterschriften