Sammlung der Rechtsprechung

SCHLUSSANTRÄGE DES GENERALANWALTS
HENRIK SAUGMANDSGAARD ØE
vom 3. Mai 2018 [1]

Rechtssache C-207/16

Ministerio Fiscal

(Vorabentscheidungsersuchen der Audiencia Provincial de Tarragona [Regionalgericht Tarragona, Spanien])

„Vorlage zur Vorabentscheidung – Elektronische Kommunikation – Verarbeitung personenbezogener Daten – Recht auf Privatsphäre und Recht auf den Schutz solcher Daten – Richtlinie 2002/58/EG – Art. 1 und Art. 15 Abs. 1 – Charta der Grundrechte der Europäischen Union – Art. 7 und 8 und Art. 52 Abs. 1 – Im Rahmen der Bereitstellung elektronischer Kommunikationsdienste erhobene Daten – Antrag auf Zugang einer Polizeibehörde zum Zwecke strafrechtlicher Ermittlungen – Grundsatz der Verhältnismäßigkeit – Begriff der ‚schweren Straftat', die einen Eingriff in Grundrechte rechtfertigen kann – Kriterien der Schwere – Strafmaß – Mindestmaß"

I. Einführung

1. Diese Vorlage zur Vorabentscheidung betrifft die Auslegung des Begriffs der „schweren Straftaten" [2] im Sinne der aus dem Urteil Digital Rights Ireland u. a. [3] (im Folgenden: Urteil Digital Rights) und dem Urteil Tele2 Sverige und Watson u. a. [4] (im Folgenden: Urteil Tele2) hervorgegangenen Rechtsprechung des Gerichtshofs, in der dieser Begriff als Kriterium für die Beurteilung der Rechtmäßigkeit und der Verhältnismäßigkeit eines Eingriffs in die in den Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) gewährleisteten Rechte, nämlich das Recht auf Achtung des Privat- und Familienlebens und das Recht auf Schutz personenbezogener Daten, verwendet worden ist.

1 Originalsprache: Französisch.

2 Der Ausdruck ist hier ausschließlich als Bezugnahme auf Verletzungen im Bereich des Strafrechts zu verstehen.

3 Urteil vom 8. April 2014 (C-293/12 und C-594/12, EU:C:2014:238), in dem 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) mit der Begründung für ungültig erklärt hat, dass „der Unionsgesetzgeber beim Erlass der Richtlinie 2006/24 die Grenzen überschritten hat, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta einhalten musste" (Rn. 69).

4 Urteil vom 21. Dezember 2016 (C-203/15 und C-698/15, EU:C:2016:970), in dem der Gerichtshof entschieden hat, 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" (Tenor 1 und 2).

2. Die Vorlage zur Vorabentscheidung erfolgt im Rahmen eines Rechtsmittels gegen eine Gerichtsentscheidung, die Polizeibehörden die Möglichkeit verwehrt hat, sich von Mobilfunkbetreibern bestimmte Personenstandsdaten, über die sie verfügen, zur Identifizierung von Personen für Zwecke strafrechtlicher Ermittlungen übergeben zu lassen. Die angefochtene Entscheidung beruhte insbesondere auf der Erwägung, dass die der Ermittlung zugrunde liegenden Tatsachen entgegen den Anforderungen der anwendbaren spanischen Regelung keine schwere Straftat darstellten.

3. Das vorlegende Gericht möchte vom Gerichtshof wissen, wie die Schwelle der Schwere der Straftat, ab der es im Hinblick auf die genannte Rechtsprechung beim Zugang der zuständigen nationalen Behörden zu von Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten gerechtfertigt sein kann, in die durch Art. 7 und 8 der Charta geschützten Grundrechte einzugreifen, zu bestimmen ist.

4. Nachdem ich nachgewiesen habe, dass der Gerichtshof zuständig ist, über diese Vorlage zur Vorabentscheidung zu entscheiden, und dass die Vorlage zulässig ist, werde ich nachweisen, dass der Zugang zu personenbezogenen Daten unter Umständen wie denjenigen im vorliegenden Fall einen Eingriff in die genannten Grundrechte darstellt, der nicht den Fällen entspricht, in denen nach der genannten Rechtsprechung nur die Bekämpfung schwerer Straftaten geeignet ist, den Eingriff in diese Rechte zu rechtfertigen.

5. Da ich der Meinung bin, dass es in Anbetracht des besonderen Gegenstands des Ausgangsverfahrens nicht notwendig sein wird, dass der Gerichtshof die Vorlagefragen in ihrem ursprünglichen Wortlaut beantwortet, werde ich nur hilfsweise Hinweise zu den Kriterien geben, die es möglicherweise erlauben würden, den Begriff der „schweren Straftaten“ im Sinne dieser Rechtsprechung insbesondere im Hinblick auf das Kriterium des Strafmaßes zu definieren.

II. Rechtlicher Rahmen

A. Unionsrecht

6. Die 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)[5] in ihrer durch die Richtlinie 2009/136/EG[6] geänderten Fassung (im Folgenden: Richtlinie 2002/58) bestimmt in ihrer Präambel:

„(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 jener Charta niedergelegten Rechte uneingeschränkt geachtet werden.

…

5 ABl. 2002, L 201, S. 37.

6 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11).

(11) Wie die Richtlinie 95/46/EG[7] 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 [im Folgenden: EMRK] in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte [im Folgenden: EGMR] 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 [EMRK[8]] entsprechen."

7. Art. 1 („Geltungsbereich und Zielsetzung") der Richtlinie 2002/58 sieht vor:

„(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 … zu gewährleisten.

…

(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."

8. Ihr Art. 2 („Begriffsbestimmungen") sieht vor:

„Sofern nicht anders angegeben, gelten die Begriffsbestimmungen der Richtlinie 95/46/EG 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') [9] auch für diese Richtlinie.

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

a) ‚Nutzer' eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

7 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).

8 Insbesondere gemäß Art. 8 EMRK, der bestimmt:
„1. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer."

9 ABl. 2002, L 108, S. 33.

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;

…"

9. Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG") der Richtlinie 2002/58 bestimmt in Abs. 1, dass „[d]ie Mitgliedstaaten … Rechtsvorschriften erlassen [können], 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/EG 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."

B. Spanisches Recht

1. Das Gesetz 25/2007

10. Die 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 [10] (im Folgenden: Gesetz 25/2007) hat die vom Gerichtshof im Urteil Digital Rights für ungültig erklärte Richtlinie 2006/24 [11] in spanisches Recht umgesetzt.

10 BOE Nr. 251 vom 19. Oktober 2007, S. 42517.

11 Dies ergibt sich sowohl aus der Präambel dieses Gesetzes als auch aus seinen wesentlichen Bestimmungen, deren Wortlaut den entsprechenden Bestimmungen der Richtlinie 2006/24 entspricht.

11. Art. 1 des Gesetzes 25/2007 in seiner auf die dem Ausgangsrechtsstreit zugrunde liegenden Tatsachen anwendbaren Fassung 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.

…“

12. Art. 3 dieses Gesetzes zählt die von den Betreibern zu speichernden Daten auf. Gemäß Abs. 1 Buchst. a Nr. 1 Ziff. ii handelt es sich insbesondere um Daten, die für die Wiederauffindung und Identifizierung der Quelle einer Kommunikation notwendig sind, wie etwa, was die Mobiltelefonie betrifft, der Name und die Anschrift des Teilnehmers oder registrierten Benutzers.

2. Strafgesetzbuch

13. Gemäß Art. 13 Abs. 1 des spanischen Strafgesetzbuchs in seiner auf die Tatsachen des Ausgangsrechtsstreits anwendbaren Fassung sind „[s]chwere Straftaten … Straftaten, die nach dem Gesetz mit schwerer Strafe bedroht sind“.

14. Art. 33 dieses Gesetzbuchs lautet:

„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;

…“

3. Strafprozessordnung

15. Die Strafprozessordnung wurde 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[12] (im Folgenden: Organgesetz 13/2015) geändert.

12 BOE Nr. 239 vom 6. Oktober 2015, S. 90192.

16. Durch dieses am 6. Dezember 2015 in Kraft getretene Gesetz wird der Bereich des Zugangs zu den von Betreibern elektronischer Kommunikationsdienste in Verbindung mit telefonischen und telematischen Kommunikationsvorgängen gespeicherten Daten in die Strafprozessordnung aufgenommen.

17. Nach dem Wortlaut von Art. 579 Abs. 1 der Strafprozessordnung in seiner aus diesem Gesetz hervorgegangenen Fassung kann „[d]as Gericht … 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 Buchst. j („Daten in automatisierten Archiven der Dienstleistungserbringer") desselben Gesetzes bestimmt:

„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."

III. Ausgangsrechtsstreit, Vorlagefragen und Verfahren vor dem Gerichtshof

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

20. Mit Schreiben vom 27. Februar 2015 beantragte die Kriminalpolizei beim Juzgado de Instrucción nº 3 de Tarragona (Ermittlungsrichter Nr. 3 von Tarragona, Spanien, im Folgenden: Ermittlungsrichter), die Anordnung gegenüber verschiedenen Telefonanbietern zu erlassen, zum einen die unter der IMEI [13] des gestohlenen Mobiltelefons zwischen dem 16. und dem 27. Februar 2015 aktivierten Telefonnummern und zum anderen die persönlichen Daten der Inhaber oder Nutzer der mit den unter dieser IMEI aktivierten Telefonnummern korrespondierenden SIM-Karten mitzuteilen [14].

21. Mit Beschluss vom 5. Mai 2015 lehnte der Ermittlungsrichter die Anordnung der beantragten Maßnahme mit den Begründungen ab, dass die Maßnahme zur Ermittlung der für den Raub Verantwortlichen wenig geeignet sei, und dass das Gesetz 25/2007 die Übermittlung gespeicherter Daten durch die Mobilfunkbetreiber jedenfalls auf schwere Straftaten beschränke – nämlich jene, die nach dem spanischen Strafgesetzbuch [15] mit einer Freiheitsstrafe von mehr als fünf Jahren gestraft würden –, der hier in Rede stehende Sachverhalt aber nicht als schwere Straftat eingestuft werde.

22. Das Ministerio Fiscal (Staatsanwaltschaft), die einzige Partei des Verfahrens, legte dagegen bei der Audiencia Provincial de Tarragona (Regionalgericht Tarragona, Spanien) Berufung ein und machte geltend, dass die Übermittlung der angeforderten Daten aufgrund des Wesens des untersuchten Sachverhalts und einer einen ähnlichen Fall betreffenden Entscheidung des Tribunal Supremo (Oberster Gerichtshof, Spanien) hätte gebilligt werden müssen [16].

23. Durch Beschluss vom 9. Februar 2016 ordnete das Berufungsgericht als vorläufige Maßnahme gegenüber den Mobilfunkbetreibern die Fortdauer der Speicherung der vom streitigen Antrag betroffenen Daten an.

24. Der Vorlageentscheidung dieses Gerichts ist zu entnehmen, dass der spanische Gesetzgeber nach Ergehen der angefochtenen Entscheidung mit dem Organgesetz 13/2015 [17] zwei alternative Kriterien für die Bestimmung der Schwere einer Straftat eingeführt habe. Das erste sei ein materielles Kriterium, das an Verhaltensweisen von besonderer und erheblicher kriminogener Relevanz anknüpft, die Individual- und Kollektivrechtsgüter besonders schädigen [18]. Das zweite sei ein normativ-formales Kriterium, das ausschließlich auf der für die den Gegenstand der Untersuchung bildende Straftat vorgesehenen Strafe beruhe. Der Strafrahmen von mindestens drei Jahren Freiheitsentzug, den Letzteres vorsehe, könne jedoch eine deutliche Mehrheit der Straftypen umfassen. Außerdem stellt das vorlegende Gericht fest, dass das staatliche Interesse am Schutz der Bürger und an der Bestrafung von rechtswidrigem Verhalten keinen unverhältnismäßigen Eingriff in die Grundrechte der Menschen rechtfertigen könne.

13 IMEI ist die Abkürzung für „International Mobile Equipment Identity“ (internationale Identifikation für Mobilgeräte). Die IMEI ist ein aus 15 Ziffern bestehender einmaliger Identifikationskode, der im Allgemeinen im Inneren des Batteriefachs des Mobiltelefons sowie auf der beim Kauf des Geräts übergebenen Verpackung und Rechnung eingetragen ist.

14 Die spanische Regierung gibt an, dass dieser Antrag vier Telefongesellschaften betraf und erklärte, dass wenn die IMEI das Telefonnetz einer dieser Gesellschaften genutzt hätte, dieses Netz aber von einem virtuellen Mobilfunkbetreiber betrieben worden wäre, auch die genannten, von Letzterem erhobenen Daten herauszugeben gewesen wären.

15 Siehe die oben in Nrn. 13 und 14 dieser Schlussanträge genannten Bestimmungen.

16 Vgl. Urteil der Sala de lo Penal (Kammer für Strafsachen) vom 26. Juli 2010 (Nr. 745/2010, ES:TS:2010:4200), abrufbar unter folgender Internetadresse: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=5697924&links=&optimize=20100812&publicinterface=true.

17 Siehe Nrn. 15 ff. dieser Schlussanträge. Nach Ansicht des vorlegenden Gerichts ist diese Reform für das Vorabentscheidungsersuchen offensichtlich einschlägig. In der mündlichen Verhandlung hat die spanische Regierung erklärt, dass die neue Regelung auf den vorliegenden Fall anwendbar sei.

18 Nämlich terroristische Straftaten und Straftaten, die im Rahmen einer kriminellen Gruppe oder Organisation begangen werden.

25. Daraufhin hat die Audiencia Provincial de Tarragona (Regionalgericht Tarragona) mit Entscheidung vom 6. April 2016, beim Gerichtshof eingegangen am 14. April 2016, 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 [Digital Rights] als Standards für die strikte Kontrolle der [durch dieses Urteil für ungültig erklärten] Richtlinie herangezogen hat, vereinbar ist, wie hoch muss dann die Mindeststrafe sein? Wäre eine allgemeine Grenze von drei Jahren Freiheitsentzug zulässig?

26. Durch Beschluss des Präsidenten vom 23. Mai 2016 ist das Verfahren vor dem Gerichtshof in Erwartung der Verkündung des Urteils des Gerichtshofs in den verbundenen Rechtssachen Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, ausgesetzt worden.

27. Auf Nachfrage des Gerichtshofs nach Verkündung dieses Urteils am 21. Dezember 2016[19] hat das vorlegende Gericht mitgeteilt, dass es sein Vorabentscheidungsersuchen aufrechterhalte. Nach seiner Auffassung bedurften die von ihm gestellten Vorlagefragen weiterhin einer Beantwortung, weil das genannte Urteil zwar Beispiele schwerer Straftaten genannt habe[20], jedoch nicht mit der erforderlichen Klarheit den materiellen Inhalt des Konzepts der Schwere der Straftat, das als Kriterium zur Beurteilung der Rechtmäßigkeit eines Eingriffs fungieren könnte, definiere. Dieses Konzept berge jedoch das Risiko, dass die staatlichen Behörden die normativen Anforderungen an die Speicherung von Daten und den Zugang zu ihnen in einer Weise sehr weit fassen, die nicht im Einklang mit den im Urteil Tele2 genannten Grundrechten steht. So habe der spanische Gesetzgeber mittels des Organgesetzes 13/2015 trotz der Kriterien im Urteil Digital Rights[21] den Schweregrad der Straftatbestände, bei denen die Speicherung und die Weitergabe von personenbezogenen Daten zulässig sind, gegenüber der Vorgängerregelung im Gesetz 25/2007 spürbar herabgesetzt.

28. Nach dieser Antwort ist das Verfahren vor dem Gerichtshof am 16. Februar 2017 wieder aufgenommen worden. Die Regierungen Spaniens, Tschechiens, Estlands, Irlands, Frankreichs, Lettlands, Ungarns, Österreichs und des Vereinigten Königreichs sowie die Europäische Kommission haben daraufhin schriftliche Erklärungen abgegeben.

29. Im Hinblick auf die mündliche Verhandlung hat der Gerichtshof der spanischen Regierung Fragen zur schriftlichen Beantwortung gestellt, die diese am 9. Januar 2018 beantwortet hat. Außerdem hat er allen Parteien im Sinne von Art. 23 der Satzung des Gerichtshofs der Europäischen Union Fragen zur mündlichen Beantwortung gestellt.

19 Vgl. Fn. 4 der vorliegenden Schlussanträge.

20 Vgl. Rn. 103 des Urteils Tele2, wo „[die organisierte] Kriminalität und [der] Terrorismus“ genannt sind. Ich wiese darauf hin, dass die gleiche doppelte Illustration in den Rn. 24 und 51 des Urteils Digital Rights im offensichtlichen Zusammenhang mit den Erwägungsgründen 7 und 10 der Richtlinie 2006/24, die dieses Urteil für ungültig erklärt hat, genannt wurde.

21 Das vorlegende Gericht nennt insbesondere Rn. 60 des Urteils Digital Rights, in der der Gerichtshof feststelle, dass „die Richtlinie 2006/24 kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen. Die Richtlinie 2006/24 nimmt im Gegenteil in ihrem Art. 1 Abs. 1 lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten schweren Straftaten Bezug.“

30. In der mündlichen Verhandlung am 29. Januar 2018 haben die spanische Staatsanwaltschaft und die Regierungen Spaniens, Tschechiens, Dänemarks, Estlands, Irlands, Frankreichs, Lettlands, Polens und des Vereinigten Königreichs sowie die Kommission mündlich Stellung genommen.

IV. Bewertung

A. Vorbemerkungen

31. Bevor ich die vom vorliegenden Vorabentscheidungsersuchen aufgeworfenen Fragen eingehend prüfe, halte ich es für notwendig, einige Bemerkungen zu seinem besonderen Gegenstand zu machen.

32. *Erstens* stelle ich in Anbetracht der Hinweise in der Vorlageentscheidung sowie der von der spanischen Regierung gegebenen zusätzlichen Informationen fest, dass der *Ausgangsrechtsstreit* erhebliche Besonderheiten aufweist, die ihn insbesondere von den Umständen der Rechtssachen unterscheiden, die zu den Urteilen Digital Rights und Tele2 geführt haben [22].

33. Der hier fragliche Antrag der Polizeibehörde ist nämlich *ausschließlich* auf die Erlangung von Daten gerichtet, die es ermöglichen, die Inhaber oder Nutzer der Telefonnummern, die zu den SIM-Karten gehören, die sich in dem gestohlenen Mobiltelefon befanden, zu identifizieren [23]. Außerdem steht fest, dass dieser Antrag einen klar definierten und kurzen Zeitraum, nämlich etwa zwölf Tage, betrifft [24].

34. Unter diesen Umständen ist die Anzahl der möglicherweise von der streitigen Maßnahme Betroffenen nicht unbegrenzt, sondern beschränkt. Außerdem sind diese Personen nicht irgendwelche Inhaber einer SIM-Karte, sondern Personen mit einem speziellen Profil, denn es handelt sich um Personen, die das gestohlene Telefon nach seiner Entwendung verwendet haben oder es sogar noch besitzen, und bei denen der Verdacht naheliegt, dass sie selbst die Täter sind oder mit diesen in Verbindung stehen.

35. Darüber hinaus handelt es sich bei den betreffenden Daten nicht um jede Art „personenbezogener Daten“ [25], die von Betreibern elektronischer Kommunikationsdienste gespeichert werden, sondern nur um Daten über die Identität der genannten Personen, nämlich ihren Vornamen, ihren Namen und gegebenenfalls ihre Anschrift [26], also um Daten, die als „Kontaktdaten“ bezeichnet werden können. Andere Informationen über diese Personen, die möglicherweise in den Archiven dieser Betreiber vorhanden sein könnten [27], sind meines Erachtens vom Ausgangsverfahren nicht betroffen.

22 Vgl. hierzu insbesondere die Fn. 3 und 4 der vorliegenden Schlussanträge.

23 Meines Erachtens handelt es sich bei den in diesem Antrag genannten „Inhabern oder Nutzern“ notwendig um registrierte oder zumindest identifizierbare Teilnehmer (siehe auch Fn. 25 der vorliegenden Schlussanträge) und nicht um Personen, die eine SIM-Karte gekauft haben, ohne eine Spur zu hinterlassen.

24 Siehe Nr. 20 der vorliegenden Schlussanträge.

25 Nach der Definition in Art. 2 Buchst. a der Richtlinie 95/46, auf die Art. 2 der Richtlinie 2002/58 verweist, bezeichnen „personenbezogene Daten“ „alle Informationen über eine bestimmte oder bestimmbare natürliche Person“, wobei klargestellt wird, dass „als bestimmbar … eine Person angesehen [wird], die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“. Der Gerichtshof hat erklärt, dass „sich die Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft“ (vgl. insbesondere Urteil vom 17. Oktober 2013, Schwarz, C-291/12, EU:C:2013:670, Rn. 26), und dass der Anwendungsbereich der Richtlinie sehr weit ist (vgl. insbesondere Urteil vom 20. Dezember 2017, Nowak, C-434/16, EU:C:2017:994, Rn. 33).

26 Gemäß der spanischen Regierung ist die Anschrift der betroffenen Personen nicht explizit angefragt worden.

27 Informationen wie etwa der Personenstand einer Person, die Nummer ihres Personalausweises, ihre Bankverbindungen und gegebenenfalls ihr Telefonanschluss.

36. Außerdem ist das hier verfolgte Ziel in meinen Augen die Sammlung von Informationen, die nicht eine Lokalisierung oder Nachrichten als solche [28], sondern natürliche Personen betreffen, die gesucht werden, weil sie einen elektronischen Kommunikationsdienst mit Hilfe eines gestohlenen Telefons genutzt haben, selbst wenn sie keinen konkreten Telefonanruf getätigt haben. Wie sich aus den Erklärungen der spanischen Staatsanwaltschaft gegenüber dem Gerichtshof ergibt, können die angefragten personenbezogenen Daten, die sich aus der Herstellung eines Zusammenhangs zwischen einer bestimmten SIM-Karte und der IMEI-Nummer des gestohlenen Geräts ergeben, technisch durch eine einfache Anmeldung des Geräts bei einer Mobilfunksäule erlangt werden, auch wenn der Inhaber mit dem betreffenden Telefon keinen Anruf getätigt hat, also unabhängig von jeder Nachricht [29]. Es wird dem vorlegenden Gericht obliegen, diese Tatsachenbehauptung zu überprüfen, die mir allerdings als ausreichend plausibel erscheint, um sie vernünftigerweise für zutreffend zu halten.

37. In Anbetracht dieser Umstände weise ich bereits jetzt darauf hin, dass der Ausgangsrechtsstreit personenbezogene Daten betrifft, deren Herausgabe nicht allgemein oder undifferenziert beantragt wird, sondern gezielt für bestimmte Personen und in Bezug auf einen begrenzten Zeitraum. Außerdem scheinen die beantragten Daten auf den ersten Blick nicht besonders sensibel zu sein, auch wenn die in den Art. 7 und 8 der Charta verankerten Grundrechte gleichwohl durch den Zugang zu Daten dieser Art betroffen sein können [30].

38. *Zweitens* stelle ich fest, dass sich aus der Begründung der Vorlageentscheidung ergibt, dass die Besonderheit der in dieser Rechtssache gestellten Vorlagefragen darin besteht, dass sie nicht die Voraussetzungen der *Speicherung* von personenbezogenen Daten im Bereich der elektronischen Kommunikation betreffen, sondern die Umstände des *Zugangs* der nationalen Behörden zu solchen Daten, die von Betreibern von in diesem Bereich tätigen Diensten gespeichert worden sind [31].

39. Das vorlegende Gericht weist insbesondere darauf hin, dass gemäß Art. 588 ter Buchst. j der Strafprozessordnung eine richterliche Genehmigung für die Übermittlung der von den Dienstleistern archivierten elektronischen Daten an die zuständigen Behörden für die Verwendung im Rahmen eines Verfahrens erforderlich ist. Abs. 1 dieses Artikels bestimmt, dass solche Daten von Dienstleistungserbringern entweder im Einklang mit den einschlägigen Rechtsvorschriften oder aus eigener Initiative aus wirtschaftlichen oder anderen Gründen gespeichert worden sein können.

40. Im vorliegenden Fall sind die personenbezogenen Daten, zu denen die Polizeibehörden für Ermittlungszwecke Zugang beantragen, von den Mobiltelefonanbietern in Erfüllung einer sich aus dem spanischen Recht ergebenden Pflicht archiviert worden [32]. Das vorlegende Gericht macht hierzu keine Angaben, sein Vorabentscheidungsersuchen ist jedoch auf einen möglichen Zugang zu Daten gerichtet, die bereits gespeichert waren, und die Vereinbarkeit der Speicherung der Daten mit den Anforderungen des Unionsrechts wird im Ausgangsverfahren nicht in Frage gestellt [33]. Es ist deshalb

28 Auskünfte, die die Nummern ein- oder ausgehender Anrufe oder das Datum, die Dauer, die Häufigkeit oder sogar den Inhalt von Nachrichten betreffen könnten. Die spanische Regierung erklärt, dass die Polizei im vorliegenden Fall ausdrücklich erklärt habe, dass ihr Antrag nicht auf die Erlangung von Daten gerichtet sei, die durch das Fernmeldegeheimnis geschützt sind.

29 Die Daten könnten mit anderen Worten durch ein einfaches Einschalten des fraglichen Mobilgeräts erlangt werden, unabhängig davon, ob dieses Gerät dann von seinem Inhaber oder Besitzer im Rahmen einer bestimmten Übermittlung von Nachrichten zwischen Personen benutzt wird.

30 Siehe Nrn. 74 ff. dieser Schlussanträge.

31 Ich weise darauf hin, dass der Zugang zu personenbezogenen Daten meines Erachtens grundsätzlich nicht weniger Gefahren für die in den Art. 7 und 8 der Charta geregelten Grundrechte beinhaltet als eine Speicherung solcher Daten. Die Gefährdung könnte sogar insofern als höher angesehen werden, als der Zugang zu gespeicherten Daten die möglicherweise schädliche Nutzung dieser Daten konkretisiert.

32 Die spanische Regierung gibt an, dass der Vorname, der Name und möglicherweise die Anschrift des Inhabers einer SIM-Karte in Spanien legal gespeichert werden dürfen. Es scheint sich mir aus Art. 1 und aus Art. 3 Abs. 1 Buchst. a Nr. 1 Ziff. ii des Gesetzes 25/2007 (siehe Nrn. 10 ff. dieser Schlussanträge) zu ergeben, dass die Mobilfunkbetreiber verpflichtet sind, die im Rahmen ihrer Leistungserbringung generierten oder verarbeiteten Daten und insbesondere den Namen und die Anschrift des Teilnehmers oder registrierten Nutzers zu speichern, soweit diese Daten notwendig sind, um die Quelle einer Kommunikation wiederzufinden und zu identifizieren. Ich erinnere daran, dass sich entsprechende Anforderungen aus Art. 3 und Art. 5 Abs. 1 Buchst. a Nr. 1 Ziff. ii der Richtlinie 2006/24 ergaben, die durch dieses Gesetz umgesetzt worden ist.

33 Ein Umstand, auf den auch der Gerichtshof im Urteil vom 29. Januar 2008, Promusicae (C-275/06, EU:C:2008:54, Rn. 45 a. E.), hingewiesen hat.

meines Erachtens von der Prämisse auszugehen, dass die im Ausgangsverfahren in Rede stehenden Daten in Übereinstimmung mit den nationalen Rechtsvorschriften unter Beachtung der in Art. 15 Abs. 1 der Richtlinie 2002/58 festgelegten Voraussetzungen gespeichert worden sind; dies zu prüfen ist Sache des vorlegenden Gerichts [34].

41. In den folgenden Ausführungen werde ich auf die rechtlichen Implikationen der hier einleitend getroffenen Feststellungen zurückkommen [35].

B. Zu den von der spanischen Regierung geltend gemachten Verfahrenseinreden

42. Die spanische Regierung hat zwei Arten von Verfahrenseinreden geltend gemacht, die eine betreffend die Zuständigkeit des Gerichtshofs und die andere betreffend die Zulässigkeit des Vorabentscheidungsersuchens, über die der Gerichtshof entscheiden muss, bevor er gegebenenfalls in der Sache entscheidet.

1. Zur Zuständigkeit des Gerichtshofs im Hinblick auf den Anwendungsbereich des Unionsrechts

43. Zunächst erinnere ich daran, dass nach ständiger Rechtsprechung des Gerichtshofs die in der Unionsrechtsordnung garantierten Grundrechte und insbesondere die in den Art. 7 und 8 der Charta garantierten nur dann Anwendung finden, wenn die Fallgestaltung in den Anwendungsbereich des Unionsrechts fällt [36]. Außerdem ergibt sich aus Art. 51 Abs. 1 der Charta, dass die Bestimmungen der Charta für die Mitgliedstaaten ausschließlich „bei der Durchführung des Rechts der Union“, gemäß der Rechtsprechung des Gerichtshofs zu diesem Begriff, gelten [37]. Folglich ist, wenn eine rechtliche Situation nicht vom Unionsrecht erfasst wird, der Gerichtshof nicht zuständig, um über sie zu entscheiden, und die möglicherweise angeführten Bestimmungen der Charta können als solche diese Zuständigkeit nicht begründen [38].

44. Im vorliegenden Fall betreffen die vom vorlegenden Gericht gestellten Frauen ausschließlich die Art. 7 und 8 der Charta sowie die „[Verfassungsgrundsätze] der Union, die der Gerichtshof in seinem Urteil [Digital Rights] herangezogen hat“. Das vorlegende Gericht ist jedoch der Meinung, dass die auf den Schutz personenbezogener Daten anwendbaren Richtlinien wie die Richtlinie 95/46 und die Richtlinie 2002/58 die von Art. 51 Abs. 1 der Charta geforderte Verbindung zwischen dem Ausgangsrechtsstreit und dem Unionsrecht herstellen.

45. Insoweit stelle ich *erstens* fest, dass die spanische Regierung in der Hauptsache geltend macht, der Gerichtshof sei nicht zuständig, über diese Vorlage zur Vorabentscheidung zu entscheiden, weil diese nicht die Anwendung des Unionsrechts betreffe. Sie macht insbesondere geltend, der Ausgangsrechtsstreit sei vom Anwendungsbereich des Unionsrechts ausgeschlossen, weil er einen Zugang der Polizei zu Daten im Rahmen einer Ermittlung betreffe, der einem Richtervorbehalt

34 In diesem Sinne Urteil vom 19. April 2012, Bonnier Audio u. a. (C-461/10, EU:C:2012:219, Rn. 37).

35 Insbesondere was die Zuständigkeit des Gerichtshofs und die Antwort auf die erste Vorlagefrage betrifft, siehe jeweils Nrn. 43 ff. und Nrn. 70 ff. dieser Schlussanträge.

36 Vgl. insbesondere Urteil vom 16. Mai 2017, Berlioz Investment Fund (C-682/15, EU:C:2017:373, Rn. 49 und die dort angeführte Rechtsprechung).

37 Vgl. insbesondere Urteil vom 6. Oktober 2016, Paoletti u. a. (C-218/15, EU:C:2016:748, Rn. 14 ff.).

38 Vgl. insbesondere Urteil vom 1. Dezember 2016, Daouidi (C-395/15, EU:C:2016:917, Rn. 63).

unterliege, was eine Tätigkeit des Staates im Bereich des Strafrechts sei [39], und falle deshalb unter die in Art. 1 Abs. 3 der Richtlinie 2002/58 sowie in Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 geregelten Ausnahmen [40]. In der mündlichen Verhandlung hat die Regierung des Vereinigten Königreichs erklärt, sie teile diesen Standpunkt der spanischen Regierung.

46. Ich bin jedoch der Meinung, dass die Richtlinie 2002/58 auf nationale Maßnahmen wie die im Ausgangsrechtsstreit streitigen anwendbar ist. Der Gerichtshof hat nämlich im Urteil Tele2 bereits entschieden, dass die nationalen Regelungen über die Aufbewahrung von Daten für Zwecke der Kriminalitätsbekämpfung in den Geltungsbereich der Richtlinie fallen, und zwar nicht nur, soweit sie die Pflichten der Anbieter von elektronischen Kommunikationsdiensten definieren, sondern auch, soweit sie den Zugang der nationalen Behörden zu den in diesem Rahmen gespeicherten Daten regeln [41]. Der Kommission folgend bin ich der Meinung, dass die in diesem Urteil genannten Erwägungen auf die im vorliegenden Fall anwendbaren nationalen Regelungen, nämlich diejenigen, die sich aus dem Gesetz 25/2007 in Verbindung mit der spanischen Strafprozessordnung in ihrer durch das Organgesetz 13/2015 geänderten Fassung ergeben [42], und damit auf den Gegenstand des Ausgangsverfahrens übertragbar sind.

47. Ich möchte hinzufügen, dass einerseits personenbezogene Daten, die *unmittelbar* im Rahmen der – hoheitlichen [43] – Tätigkeiten des Staates in einem Bereich des Strafrechts verarbeitet werden [44], und andererseits solche Daten, die im Rahmen von – wirtschaftlichen – Tätigkeiten eines Anbieters von elektronischen Kommunikationsdiensten verarbeitet werden, und die *danach* von den zuständigen staatlichen Behörden verwendet werden [45], nicht verwechselt werden dürfen. Außerdem weise ich darauf hin, dass der Gerichtshof vor Kurzem um Vorabentscheidung insbesondere über die Auslegung von Art. 1 Abs. 3 der Richtlinie 2002/58 im Kontext einer Nutzung von Daten durch die Sicherheits- und Nachrichtendienste eines Mitgliedstaats ersucht wurde, die ihnen von solchen Anbietern als Massendaten übermittelt werden mussten [46]; über diese Problematik ist meines Erachtens in der vorliegenden Rechtssache nicht zu entscheiden [47].

48. *Zweitens* stelle ich fest, dass andere Fragen in Bezug auf den *Anwendungsbereich der Richtlinie 2002/58* aufgeworfen worden sind, von denen die Zuständigkeit des Gerichtshofs in Anbetracht der *Art der im Ausgangsverfahren streitigen Daten* abhängt.

39 Nach Ansicht der spanischen Regierung handelt es sich hier um eine Ausübung des Rechts zu strafen (*ius puniendi*) durch die staatlichen Behörden. Vgl. hierzu die Schlussanträge des Generalanwalts Campos Sánchez-Bordona in der Rechtssache Breyer (C-582/14, EU:C:2016:339, Nrn. 86 bis 92).

40 Die in diesen Bestimmungen genannten Grundsätze werden auch im elften Erwägungsgrund der Richtlinie 2002/58 erwähnt, der auf Art. 15 Abs. 1 dieser Richtlinie verweist (siehe Nrn. 6 und 7 dieser Schlussanträge).

41 Vgl. Rn. 72 bis 81 des Urteils Tele2. Vgl. hierzu auch meine Schlussanträge in den verbundenen Rechtssachen Tele2 Sverige u. a. (C-203/15 und C-698/15, EU:C:2016:572, Nrn. 88 bis 97 und Nr. 124).

42 Vgl. insbesondere Art. 1 Abs. 1 des Gesetzes 25/2007 und Art. 579 Abs. 1 der Strafprozessordnung, wiedergegeben in den Nrn. 11 und 17 dieser Schlussanträge, sowie, zur gesetzlichen Pflicht dieser Diensteanbieter, Nr. 40 dieser Schlussanträge.

43 „Hoheitliche" Tätigkeiten des Staates betreffen Aufgaben, die dem Staat und seinen Untergliederungen vorbehalten sind und die er nicht an private Stellen delegieren kann, nämlich insbesondere Tätigkeiten im Zusammenhang mit der Justiz, der Polizei und der Armee.

44 Wie etwa Daten, die von Polizei- und Justizbehörden zur Ermittlung von Straftätern verarbeitet werden (z. B. Daten, die von der Polizei bei einer von einem Ermittlungsrichter angeordneten Telefonabhörung erhoben und verarbeitet werden).

45 Wie etwa Adressdaten von Nutzern von Telefondiensten, die im Rahmen einer strafrechtlichen Ermittlung wie im Ausgangsrechtsstreit verarbeitet werden.

46 Vgl. die Vorlageentscheidung in der Rechtssache Privacy International (C-623/17), die insbesondere Bezug nimmt auf die Urteile vom 30. Mai 2006, Parlament/Rat und Kommission (C-317/04 und C-318/04, EU:C:2006:346, Rn. 56 bis 59), und vom 10. Februar 2009, Irland/Parlament und Rat (C-301/06, EU:C:2009:68, Rn. 88 und 91), aus denen hervorgehe, dass die Verarbeitung von Fluggastdatensätzen, die Gegenstand des erstgenannten Urteils waren, nicht für die Erbringung einer Dienstleistung, sondern zur Wahrung der öffentlichen Sicherheit erforderlich gewesen sei und daher von der Richtlinie 95/46 nicht erfasst gewesen sei.

47 Zum einen betrifft der Ausgangsrechtsstreit hier nicht die Übermittlung von Massen-, sondern von ganz bestimmten Daten und zum anderen können meiner Meinung nach die Erwägungen des Gerichtshofs im Urteil Tele2 auf den vorliegenden Fall übertragen werden, wie ich in Nr. 46 der vorliegenden Schlussanträge aufgezeigt habe.

49. Wie ich bereits erklärt habe [48], ergibt sich aus den zur Akte gereichten Unterlagen, dass der streitige Antrag auf Zugang auf die Erlangung von Informationen über die Identität der Inhaber oder Nutzer der Telefonnummern, die den SIM-Karten entsprechen, die mit Hilfe des gestohlenen Mobiltelefons aktiviert worden sind, gerichtet ist, um die Personen, die im Besitz dieses Geräts waren, aufzufinden, und nicht auf die Erlangung von Auskünften über möglicherweise mit diesem Gerät getätigte Anrufe.

50. Mit anderen Worten bezieht sich der vorliegende Ausgangsrechtsstreit, auch wenn in Anbetracht der spanischen Regelung ein größerer Strauß von personenbezogenen Daten potenziell hätte betroffen sein können [49], auf Daten, die ausschließlich die Identität der „Nutzer" im Sinne von Art. 2 Abs. 2 Buchst. a der Richtlinie 2002/58 betreffen, und nicht auf Daten über irgendeinen „Standort" [50] im Sinne von Art. 2 Abs. 2 Buchst. c dieser Richtlinie und auch nicht auf „Nachrichten" als solche im Sinne von Art. 2 Abs. 2 Buchst. d dieser Richtlinie [51].

51. Nach Ansicht der spanischen Staatsanwaltschaft, der Regierungen Spaniens, Dänemarks, Irlands, Lettlands und des Vereinigten Königreichs sowie der Kommission sollten Informationen wie die hier streitigen, soweit sie isoliert betrachtet werden, also unabhängig von den gegebenenfalls übermittelten Nachrichten, grundsätzlich nicht vom Begriff der „Verkehrsdaten" im Sinne von Art. 2 Abs. 2 Buchst. b erfasst sein, der diese als „Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden", definiert [52].

52. Zwar scheinen die hier von den Polizeibehörden angeforderten Identifikationsdaten nicht den „Verkehr" von Nachrichten im wörtlichen Sinne zu betreffen, da diese Daten auch erlangt werden können, wenn möglicherweise gar kein Anruf mit dem gestohlenen Gerät getätigt worden ist, und also auch dann, wenn in dem betreffenden Zeitraum keine Nachrichten zwischen Personen von einem Mobiltelefonanbieter übermittelt worden sind [53].

53. Gleichwohl bin ich der Meinung, dass ein Rechtsstreit wie derjenige, der dem Ausgangsverfahren zugrunde liegt, in den Anwendungsbereich der Richtlinie 2002/58 fällt, wenn die vorliegend betroffene Verarbeitung von Informationen im Zusammenhang mit SIM-Karten und ihren Inhabern aus wirtschaftlichen Gründen für die Erbringung von elektronischen Kommunikationsdiensten notwendig ist [54], und sei es auch nur für die Abrechnung der erbrachten Dienste [55], unabhängig davon, ob im Rahmen dieser Leistung Anrufe getätigt worden sind oder nicht.

54. Was Art. 1 Abs. 1 und Art. 3 der Richtlinie 2002/58 anbelangt [56], teile ich die insbesondere von der Kommission geäußerte Auffassung, dass die Richtlinie die Verarbeitung personenbezogener Daten im Rahmen der Erbringung von elektronischen Kommunikationsdiensten umfassend regeln soll, so dass auch Daten über die Identität der Nutzer solcher Dienst wie die hier streitigen, und nicht nur Daten

48 Siehe Nrn. 33 ff. dieser Schlussanträge.

49 Vgl. insbesondere Art. 1 Abs. 2 des Gesetzes 25/2007 und Art. 579 Abs. 1 der Strafprozessordnung.

50 Der Antrag der Polizeibehörden ist nicht auf die Bestimmung des geografischen Standorts des gestohlenen Geräts oder der Personen gerichtet, die es in Besitz hatten, sondern nur auf die Identität dieser Personen.

51 Die Bestimmungen dieses Art. 2 sind in Nr. 8 dieser Schlussanträge wiedergegeben.

52 Verkehrsdaten, die in Art. 6 der Richtlinie 2002/58 geregelt sind.

53 Siehe Nr. 36 dieser Schlussanträge.

54 Elektronische Kommunikationsdienste werden in Art. 2 Buchst. c der Richtlinie 2002/21 (die in diesem Bereich den gemeinsamen Rechtsrahmen regelt) als „gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen …", definiert.

55 Die Tatsache, dass die Verarbeitung von Daten insbesondere in Bezug auf Teilnehmer für die Abrechnung der Dienste notwendig sein kann, wird in mehreren Bestimmungen der Richtlinie 2002/58 erwähnt (insbesondere Erwägungsgründe 26, 27 und 29, Art. 2 Abs. 2 Buchst. g und Art. 6 Abs. 2 und 5). Vgl. hierzu auch Rn. 86 des Urteils Tele2 und die dort angeführte Rechtsprechung.

56 Die Bestimmungen betreffen zum einen allgemein „die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation" und zum anderen „die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste".

über eine bestimmte Übermittlung von Nachrichten, von ihrem Anwendungsbereich erfasst sind. In Anbetracht auch der Schutzziele dieser Richtlinie, die im Wesentlichen im Schutz der durch die Charta gewährleisteten Grundrechte bestehen [57], bin ich deshalb der Meinung, dass der Begriff der „Nachricht" im Sinne dieser Richtlinie weit zu verstehen ist und dass der in dieser Richtlinie geregelte Grundsatz der Vertraulichkeit der Kommunikation [58] vorliegend betroffen ist.

55. Ich bin außerdem der Meinung, dass die Auslegung durch ein früheres Urteil des Gerichtshofs, in dem er bereits anerkannt hat, dass ein Rechtsstreit über die Übermittlung der Namen und Anschriften der Nutzer eines elektronischen Kommunikationsdienstes vom Anwendungsbereich der Richtlinie 2002/58 erfasst ist [59], bestätigt wird. Außerdem betrifft Art. 12 dieser Richtlinie über Teilnehmerverzeichnisse meines Erachtens bestimmte Daten dieser Art [60] und ist der 15. Erwägungsgrund Ausdruck eines weiten Verständnisses des Begriffs der „Nachricht", da insbesondere „Adressen …, die der Absender einer Nachricht … bereitstellt", einbezogen werden [61].

56. Außerdem entspricht ein solcher Ansatz der Rechtsprechung des EGMR in diesem Bereich [62], wobei daran zu erinnern ist, dass die Präambel der Richtlinie 2002/58 darauf hinweist, dass sie die Vertraulichkeit der Kommunikation und das Recht der Nutzer auf Privatleben im Einklang mit der EMRK, wie sie von diesem Gericht ausgelegt wird, gewährleisten soll [63], auch wenn diese Konvention nicht formell Bestandteil der Unionsrechtsordnung ist [64].

57. Ich bin deshalb der Meinung, dass ein Rechtsstreit wie derjenige im Ausgangsverfahren in den sachlichen Anwendungsbereich der Richtlinie 2002/58 fällt und dass die von der spanischen Regierung erhobene Einrede der Unzuständigkeit zurückgewiesen werden muss.

58. Der Vollständigkeit halber weise ich jedoch darauf hin, dass für den Fall, dass die Richtlinie 2002/58 in einer solchen Situation nicht für anwendbar gehalten würde, die sowohl vom vorlegenden Gericht als auch von der spanischen Regierung genannte Richtlinie 95/46 die Zuständigkeit des Gerichtshofs zur Entscheidung in der vorliegenden Rechtssache nicht begründen könnte.

57 Vgl. Erwägungsgründe 2, 7 und 11 sowie Art. 1 Abs. 1 und Art. 15 Abs. 3 der Richtlinie 2002/58.

58 Vgl. 21. Erwägungsgrund sowie Art. 1 Abs. 1 und, speziell zur Vertraulichkeit der Kommunikation, Art. 5 der Richtlinie 2002/58.

59 Vgl. Urteil vom 29. Januar 2008, Promusicae (C-275/06, EU:C:2008:54, Rn. 29 bis 31 und 45).

60 Zur Auslegung dieses Art. 12 vgl. insbesondere Urteil vom 15. März 2017, Tele2 (Netherlands) u. a. (C-536/15, EU:C:2017:214, Rn. 33 ff. und die dort angeführte Rechtsprechung).

61 Nach dem Wortlaut dieses 15. Erwägungsgrundes kann „[e]ine Nachricht … 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".

62 Der Begriff der Daten über das Privatleben einer Person im Sinne von Art. 8 EMRK (wiedergegeben in Fn. 8 dieser Schlussanträge) wird vom EGMR weit ausgelegt (vgl. insbesondere EGMR, 13. Februar 2018, Ivashchenko gegen Russland, CE:ECHR:2018:0213JUD006106410, §§ 63 ff.), wie bereits festgestellt wurde (vgl. Urteil vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 59 und die dort angeführte Rechtsprechung des EGMR).

63 Vgl. Erwägungsgründe 3, 11 und 24 der Richtlinie 2002/58.

64 Vgl. insbesondere Urteil Tele2 (Rn. 120, wo eine Analogie zu der Rechtsprechung des EGMR gebildet wird, sowie Rn. 126 ff., wo an das Verhältnis der Union zur EMRK erinnert wird).

59. Zwar ist die Richtlinie 95/46, wie die Kommission erklärt, der allgemeine Rechtsakt im Bereich der Verarbeitung personenbezogener Daten [65], die vom vorlegenden Gericht gestellten Fragen wären jedoch meines Erachtens nicht entscheidungserheblich, wenn sie nur unter diesem Gesichtspunkt geprüft würden, da sie auf die Bestimmung der Schwelle gerichtet sind, ab der Straftaten im Sinne der Urteile Digital Rights und Tele2, die nicht die Auslegung dieser Richtlinie betrafen, als „schwer" angesehen werden [66].

2. Zur Zulässigkeit des Vorabentscheidungsersuchens

60. Hilfsweise macht die spanische Regierung geltend, dass das Vorabentscheidungsersuchen für den Fall, dass sich der Gerichtshof zur Beantwortung der gestellten Fragen für unzuständig erklärt, für unzulässig erklärt werden müsse, und zwar aus zwei Gründen.

61. *Erstens* trägt diese Regierung vor, dass das vorlegende Gericht *den rechtlichen Rahmen der Union*, über den der Gerichtshof entscheiden soll, *nicht klar bezeichne*.

62. Insoweit erinnere ich an die ständige Rechtsprechung, nach der der Gerichtshof im Rahmen der durch Art. 267 AEUV geschaffenen Zusammenarbeit eine Entscheidung über Vorlagefragen, für die eine Vermutung der Entscheidungserheblichkeit gilt, nur verweigern darf, wenn die erbetene Auslegung einer Vorschrift des Unionsrechts oder die erbetene Beurteilung ihrer Gültigkeit 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 oder rechtlichen Angaben verfügt, die für eine sachdienliche Beantwortung der Frage erforderlich sind [67].

63. Ich bin jedoch der Ansicht, dass die Rüge der spanischen Regierung im vorliegenden Fall unbegründet ist. Angesichts der Angaben des vorlegenden Gerichts bin ich der Meinung, dass dieses die seines Erachtens entscheidungserheblichen Bestimmungen des Unionsrechts hinreichend genau bezeichnet hat. Ich erinnere daran, dass zum einen die gestellten Fragen insbesondere die Art. 7 und 8 der Charta betreffen, und dass zum anderen das vorlegende Gericht ausführt, dass die Richtlinien 95/46 und 2002/58 den notwendigen Zusammenhang zwischen den im Ausgangsverfahren anwendbaren nationalen Regelungen und dem Unionsrecht herstellen [68], und dass schließlich die Richtlinie 2002/58, wie sich aus ihrem zweiten Erwägungsgrund ergibt, insbesondere darauf gerichtet ist, die uneingeschränkte Achtung der in den Art. 7 und 8 der Charta genannten Rechte zu gewährleisten [69].

64. Es ist außerdem irrelevant, dass ein Teil des in der Vorlageentscheidung genannten spanischen Rechts, nämlich das Gesetz 25/2007, die Umsetzung der Richtlinie 2006/24 zum Gegenstand hatte, die, nachdem sie durch das Urteil Digital Rights für ungültig erklärt worden war, aufgehoben worden ist [70]. Das vorlegende Gericht weist zu Recht darauf hin, dass es unzutreffend wäre, anzunehmen, dass die dem Gerichtshof hier vorgelegten Vorlagefragen durch diese Ungültigerklärung ihre

65 Während die Richtlinie 2002/58 den speziellen Bereich der elektronischen Kommunikation betrifft (vgl. insbesondere ihre Erwägungsgründe 4 und 10 sowie ihren Art. 1 Abs. 1 und 2).

66 Ich erinnere daran, dass der Begriff der „schweren Straftat" als Kriterium zur Beschränkung der Handlungen der Mitgliedstaaten durch die Richtlinie 2006/24 über die Vorratsspeicherung von Daten, die durch das Urteil Digital Rights für ungültig erklärt worden ist, eingeführt worden ist, und dass er danach vom Gerichtshof im Urteil Tele2 für die Auslegung der Bestimmungen der Richtlinie 2002/58 im Zusammenhang mit den nationalen Regelungen über die Speicherung und den Zugang zu Daten verwendet worden ist (siehe auch Fn. 3 und 4 dieser Schlussanträge). Daraus ergibt sich meines Erachtens, dass wenn die Richtlinie 2002/58 im vorliegenden Fall für unanwendbar erklärt würde, dieser Begriff nicht wie vom vorlegenden Gericht beantragt auszulegen wäre.

67 Vgl. insbesondere Urteile vom 16. Juni 2015, Gauweiler u. a. (C-62/14, EU:C:2015:400, Rn. 24 und 25), sowie vom 22. Februar 2018, Porras Guisado (C-103/16, EU:C:2018:99, Rn. 34).

68 Siehe auch Nr. 44 dieser Schlussanträge.

69 Vgl. ebenso Urteil Tele2 (Rn. 82).

70 Siehe auch Nr. 10 des dieser Schlussanträge. Ich stelle fest, dass die Situation in einer der Rechtssachen, die zum Urteil Tele2 geführt haben, ähnlich war (vgl. Rn. 15 und 63).

Entscheidungserheblichkeit verloren haben. Insoweit genügt die Feststellung, dass der von den Fragen betroffene Bereich, nämlich der Schutz personenbezogener Daten, in die Zuständigkeit der Union fällt, und dass der Ausgangsrechtsstreit in den Anwendungsbereich eines Unionsrechtsakts fällt, nämlich der Richtlinie 2002/58 [71], die die für ungültig erklärte Richtlinie 2006/24 ändern sollte.

65. Es ist außerdem festzustellen, dass die Parteien, die Stellungnahmen gegenüber dem Gerichtshof abgegeben haben, ganz überwiegend davon ausgehen, dass das Vorabentscheidungsersuchen in Bezug auf den im Licht der Art. 7 und 8 der Charta zu lesenden Art. 15 Abs. 1 der Richtlinie 2002/58 sowie auf der Grundlage der Lehren aus den Urteilen Digital Rights und Tele2 zu prüfen ist. Das ist auch meine Meinung, wobei ich darauf hinweise, dass die Richtlinie 2002/58 den Begriff der „Straftaten" und nicht den Begriff der „schweren Straftaten" nur in dem genannten Art. 15 Abs. 1 verwendet [72].

66. *Zweitens* macht die spanische Regierung geltend, dass *Art. 7 der Charta*, der das zentrale Element des vorliegenden Vorabentscheidungsersuchens darstelle, *nicht entscheidungserheblich sei*, weil die im Ausgangsrechtsstreit beantragte Ermittlungsmaßnahme keine Überwachung der Kommunikation betreffe und deshalb die Vertraulichkeit der Kommunikation nicht berühren könne, so dass die gestellten Fragen hypothetisch seien.

67. Meines Erachtens ist Art. 7 der Charta in der vorliegenden Rechtssache entscheidungserheblich und das Vorabentscheidungsersuchen damit nicht hypothetisch. Zwar besteht vorliegend in Anbetracht des Gegenstands der im Ausgangsverfahren streitigen Maßnahme nicht die Gefahr einer Verletzung des Rechts auf Vertraulichkeit der Kommunikation [73], eine Maßnahme dieser Art ist jedoch gleichwohl geeignet, das Recht auf Achtung des Privatlebens, das durch diese Bestimmung gewährleistet wird, zu verletzen, auch wenn diese Verletzung meiner Ansicht nach geringfügig ist [74].

68. Nach ständiger Rechtsprechung des Gerichtshofs stellt die Weitergabe personenbezogener Daten an einen Dritten, etwa eine Behörde, unabhängig von der späteren Verwendung der übermittelten Informationen einen Eingriff in das in Art. 7 der Charta verankerte Grundrecht dar. Das Gleiche gilt für die Speicherung personenbezogener Daten insbesondere durch Anbieter von elektronischen Kommunikationsdiensten und für den Zugang zu diesen Daten im Hinblick auf ihre Nutzung durch öffentliche Stellen [75].

69. Ich bin deshalb der Meinung, dass die von der spanischen Regierung erhobene Einrede der Unzulässigkeit zurückzuweisen und in der Sache über das Vorabentscheidungsersuchen zu entscheiden ist.

C. Zu den Kriterien, anhand deren die hinreichende Schwere der Straftaten als Kriterium, das einen Eingriff in die Grundrechte rechtfertigt, ermittelt werden kann (erste Frage)

70. Mit seiner ersten Frage möchte das vorlegende Gericht wissen, anhand welcher Kriterien gemäß der aus den Urteilen Digital Rights und Tele2 hervorgegangenen Rechtsprechung zu ermitteln ist, ob Straftaten hinreichend schwer sind, um im Rahmen der Speicherung personenbezogener Daten und des Zugangs zu diesen Daten einen Eingriff in die von den Art. 7 und 8 der Charta gewährleisteten Grundrechte zu rechtfertigen.

71 Siehe hierzu Nrn. 45 ff. dieser Schlussanträge.

72 Siehe Nr. 71 dieser Schlussanträge.

73 Siehe Nrn. 36 und 52 dieser Schlussanträge.

74 Zur fehlenden Schwere des Eingriffs in der vorliegenden Sache siehe Nrn. 74 ff. dieser Schlussanträge.

75 Vgl. insbesondere das Urteil Digital Rights (Rn. 26 ff.) sowie Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017 (EU:C:2017:592, Rn. 124 und die dort angeführte Rechtsprechung).

71. Insoweit erinnere ich daran, dass der Gerichtshof den Begriff der „schweren Straftaten“ im Urteil Digital Rights verwendet hat [76], gelegentlich in Verbindung mit dem Begriff der „schweren Kriminalität“ [77], um den Zweck und die Verhältnismäßigkeit des Eingriffs in die genannten Grundrechte, der sich aus den Bestimmungen des Unionsrechts zu personenbezogenen Daten, insbesondere jenen der Richtlinie 2006/24 ergab, zu prüfen. Dieser Begriff, der in der Richtlinie 2002/58 nicht erscheint [78], wurde in der Richtlinie 2006/24 verwendet [79], deren Ungültigkeit Gegenstand des genannten Urteils war. Der Gerichtshof hat sodann beide Begriffe im Urteil Tele2 [80] als ein Beurteilungskriterium verwendet, nunmehr jedoch für die Vereinbarkeit mit dem Unionsrecht [81] der von den Mitgliedstaaten verabschiedeten Bestimmungen.

72. Genauer wird der Gerichtshof mit der ersten Vorlagefrage aufgefordert, zu entscheiden, ob für die Beurteilung, ob eine „schwere Straftat“ vorliegt, die einen Eingriff in die in den Art. 7 und 8 der Charta geregelten Grundrechte in Bezug auf personenbezogene Daten rechtfertigen kann, nur das Strafmaß der betreffenden Straftat zu berücksichtigen ist, oder darüber hinaus auch die besondere Schädlichkeit des deliktischen Verhaltens für Individual- oder Kollektivrechtsgüter.

73. Der Kommission folgend bin ich jedoch der Meinung, dass vor der Beantwortung dieser Frage zu prüfen ist, ob der betreffende Eingriff in einem Rechtsstreit wie demjenigen des Ausgangsverfahrens hinreichend schwer ist, damit vom Unionsrecht gefordert wird, dass dieser Eingriff mit der Bekämpfung einer schweren Straftat gerechtfertigt wird, um zulässig zu sein. Wenn dies nicht der Fall wäre, müsste der Gerichtshof die entscheidungserheblichen Bestimmungen des Unionsrechts meines Erachtens nicht in Bezug auf die vom vorlegenden Gericht gestellte Frage, sondern nach einer Umformulierung der ersten Vorlagefrage [82], soweit dies im Hinblick auf die Umstände des Ausgangsrechtsstreits notwendig ist [83], auslegen.

1. Zur Berücksichtigung der fehlenden Schwere des streitigen Eingriffs

74. *Zunächst* ist festzustellen, ob Handlungen wie jene im Ausgangsverfahren geeignet sind, die von den Art. 7 und 8 der Charta gewährleisteten Grundrechte zu verletzen und somit im Sinne der aus den Urteilen Digital Rights und Tele2 hervorgegangenen Rechtsprechung *einen Eingriff* in diese Rechte *darzustellen*.

76 Vgl. Rn. 24, 41, 49 und 57 bis 61 des Urteils Digital Rights.

77 Vgl. Rn. 41, 42 51 und 59 des Urteils Digital Rights.

78 Nur der Begriff der „Straftaten“ wird in der Richtlinie 2002/58 in ihrem Art. 15 Abs. 1 Satz 1 verwendet.

79 Sinngemäß im neunten Erwägungsgrund der Richtlinie 2006/24 sowie wörtlich im 21. Erwägungsgrund und in Art. 1 Abs. 1 der Richtlinie.

80 Vgl., in Bezug auf den Begriff der „schweren Straftaten“, Rn. 105, 106 und 119 sowie, in Bezug auf den Begriff der „schweren Kriminalität“, Rn. 102, 103, 108, 110, 111, 114, 115, 118, 125 und 134 des Urteils Tele2.

81 Nämlich mit Art. 15 Abs. 1 der Richtlinie 2002/58, wonach die Mitgliedstaaten Rechtsvorschriften erlassen können, die vom Grundsatz der Vertraulichkeit der Kommunikation und der auf sie bezogenen Verkehrsdaten abweichen, wenn dies in einer demokratischen Gesellschaft im Hinblick auf die in dieser Vorschrift genannten Ziele notwendig, angemessen und verhältnismäßig ist.

82 Die zweite Vorlagefrage wird nur hilfsweise gestellt.

83 Nach ständiger Rechtsprechung des Gerichtshofs hat der Gerichtshof, um dem vorlegenden Gericht eine für die Entscheidung des bei diesem anhängigen Rechtsstreits sachdienliche Antwort zu geben, die ihm vorgelegten Fragen gegebenenfalls umzuformulieren (vgl. insbesondere Urteil vom 22. Februar 2018, SAKSA, C-185/17, EU:C:2018:108, Rn. 28).

75. Zwar scheinen, wie die Regierungen Spaniens und Dänemarks mündlich vorgetragen haben [84] und wie ich bereits erklärt habe [85], die Daten, zu denen die mit der fraglichen strafrechtlichen Ermittlung betrauten Behörden Zugang haben möchten, weniger sensibel zu sein als bestimmte andere Arten personenbezogener Daten [86], denn der streitgegenständliche Antrag betrifft nur die Vornamen, die Namen und gegebenenfalls die Anschriften der von den Ermittlungen betroffenen Personen als Nutzer der mit dem gestohlenen Mobiltelefon, das Gegenstand dieser Ermittlungen ist, aktivierten Telefonnummern.

76. Ich bin jedoch der Ansicht, dass es für die Feststellung, ob personenbezogene Daten vom Schutz des Unionsrechts und insbesondere von der Richtlinie 2002/58 erfasst sein müssen [87], unerheblich ist, ob die vom Antrag auf Speicherung oder Übermittlung erfassten Informationen besonders sensibel sind oder nicht. Wie im Rahmen der ersten gesetzgeberischen Arbeiten in diesem Bereich festgestellt, „können alle Daten im Zusammenhang mit einer Person, selbst wenn diese scheinbar harmlos sind, bei entsprechender Verwendung sensiblen Charakter haben (eine einfache Postanschrift beispielsweise)“ [88]. Außerdem hat der Gerichtshof bereits entschieden, dass es für die Feststellung des *Bestehens eines Eingriffs* in das in Art. 7 der Charta verankerte Grundrecht „nicht darauf [ankommt], ob die übermittelten Informationen als sensibel anzusehen sind oder ob die Betroffenen durch den Vorgang irgendwelche Nachteile erlitten haben“ [89].

77. Außerdem erinnere ich daran, dass die Übermittlung personenbezogener Daten an einen Dritten, selbst an eine öffentliche Stelle wie die Kriminalpolizei, einen Eingriff in das von Art. 7 der Charta gewährleistete Grundrecht darstellt [90], und zwar auch dann, wenn diese Informationen für strafrechtliche Ermittlungen übermittelt werden, was übrigens ausdrücklich in Art. 15 Abs. 1 der Richtlinie 2002/58 geregelt ist [91]. Darüber hinaus kann eine solche Handlung auch das durch Art. 8 der Charta gewährleistete Grundrecht auf Schutz personenbezogener Daten verletzen, weil sie eine Verarbeitung personenbezogener Daten beinhaltet [92].

78. Ich bin deshalb der Meinung, dass festzustellen ist, dass eine Maßnahme wie die im Ausgangsverfahren streitige einen Eingriff in die in den Art. 7 und 8 der Charta geregelten Grundrechte darstellt.

79. *Gleichwohl* bin ich der Meinung, dass unter den vorliegenden Umständen ein wesentliches Merkmal fehlt, das der Gerichtshof berücksichtigt hat, um bei der Rechtfertigung eines Eingriffs das Bestehen einer „schweren Straftat“ – einem Begriff, dessen Definition das vorlegende Gericht beantragt – zu fordern, um vom Grundsatz der Vertraulichkeit der elektronischen Kommunikation

84 Die spanische Regierung hat darauf hingewiesen, dass die Daten, die Gegenstand des Ausgangsrechtsstreits sind, es z. B. nicht erlauben, ein Profil von der betroffenen Person zu erstellen.

85 Siehe Nrn. 35 bis 37 dieser Schlussanträge.

86 Ich erinnere daran, dass die Richtlinie 95/46 in Art. 8 besondere Regelungen über die Verarbeitung von „[personenbezogenen] Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben“ enthält. Zum Begriff der sensiblen Daten und zu ihrer Verarbeitung vgl. *Manuel de droit européen en matière de protection des données*, erarbeitet unter der Ägide der Agentur der Europäischen Union für Grundrechte und des Europarats, 2014, aktualisierte Fassung abrufbar unter der folgenden Internetadresse: https://www.coe.int/fr/web/data-protection/home, S. 46 ff. sowie S. 94 ff.

87 Der sensible Charakter bestimmter Daten wird nur im 25. Erwägungsgrund der Richtlinie 2002/58 erwähnt, ohne dass daraus abgeleitet werden könnte, dass es sich um ein allgemeines Erfordernis handelt.

88 Vgl. Mitteilung der Kommission vom 13. September 1990 zum Schutze von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und zur Sicherheit der Informationssysteme (KOM[90] 314 endg., S. 20).

89 Vgl. Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017 (EU:C:2017:592, Rn. 124 und die dort angeführte Rechtsprechung). Der EGMR hat ebenfalls in diesem Sinne geurteilt (vgl. EGMR, 16. Februar 2000, Amann gegen Schweiz, CE:ECHR:2000:0216JUD002779895, §§ 68 bis 70).

90 Siehe Nr. 68 dieser Schlussanträge. Vgl. außerdem EGMR, 8. Februar 2018, Ben Faiza gegen Frankreich (CE:ECHR:2018:0208JUD003144612, §§ 66 bis 68), über eine gerichtliche Beschlagnahme zur Erlangung von Informationen über die Verwendung eines Telefons.

91 Mit folgenden Worten: „Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten“.

92 Vgl. in diesem Sinne Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017 (EU:C:2017:592, Rn. 126 und die dort angeführte Rechtsprechung).

abweichen zu können. Das Merkmal, das meines Erachtens vorliegend *fehlt*, damit die erste Vorlagefrage in den von diesem Gericht verwendeten Worten beantwortet werden kann, ist dasjenige der *Schwere des streitigen Eingriffs*, eines Faktors, der, wenn er vorläge, die Notwendigkeit einer verstärkten Rechtfertigung bewirken würde.

80. Insoweit stelle ich fest, dass der Gerichtshof im Urteil Digital Rights die große Reichweite und die besondere Schwere des Eingriffs durch die betreffende Regelung hervorgehoben hat, indem er insbesondere festgestellt hat, „dass sich die Richtlinie 2006/24 generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckt, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen“ [93].

81. Ähnlich hat der Gerichtshof im Urteil Tele2 entschieden, dass „Art. 15 Abs. 1 der Richtlinie 2002/58/EG … 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“ [94]. In diesem Urteil wurde ein Zusammenhang hergestellt zwischen der festgestellten besonderen „Schwere des Eingriffs“ und der Notwendigkeit, eine so weitreichende Verletzung der in den Art. 7 und 8 der Charta gewährleisteten Grundrechte unter Berufung auf ein so grundlegendes Kollektivrechtsgut wie die „Bekämpfung der schweren Kriminalität“ zu rechtfertigen [95].

82. Diese Herstellung eines Zusammenhangs zwischen der Schwere des festgestellten Eingriffs und der Schwere der Gründe, die diesen Eingriff rechtfertigen können, erfolgte im Einklang mit dem Verhältnismäßigkeitsgrundsatz [96]. Außerdem hat der EGMR in seiner Rechtsprechung zu Art. 8 EMRK [97] einen vergleichbaren Zusammenhang hergestellt, wie er sich meines Erachtens aus den Urteilen Digital Rights und Tele2 ergibt.

83. Wie ich jedoch oben festgestellt habe [98] und wie die Regierungen Frankreichs und des Vereinigten Königreichs sowie die Kommission betont haben, unterscheidet sich die Art des im Ausgangsrechtsstreit streitigen Eingriffs in mehrerlei Hinsicht von denjenigen, die dem Gerichtshof in den zwei vorangegangenen Urteilen vorlagen. Die Prüfung der Vereinbarkeit einer Maßnahme wie der hier zu beurteilenden mit dem Unionsrecht hat also anders zu erfolgen.

84. Vorliegend handelt es sich nicht um eine Maßnahme in Bezug auf eine Pflicht, Verkehrs- und Standortdaten irgendeines Teilnehmers oder Nutzers, die alle elektronischen Kommunikationsmittel betreffen, allgemein und unterschiedslos zu speichern. Es handelt sich um eine gezielte Maßnahme, die auf die Möglichkeit eines Zugangs der zuständigen Behörden für die Zwecke einer strafrechtlichen

93 Rn. 57 des Urteils Digital Rights. Zu der besonderen Schwere des fraglichen Eingriffs vgl. auch Rn. 37, 39, 47, 48, 60 und 65 dieses Urteils.

94 Tenor 1 des Urteils Tele2.

95 In den Worten von Rn. 102 des Urteils Tele2 vermag „[*i*]*n Anbetracht der Schwere des Eingriffs* in die betreffenden Grundrechte durch eine nationale Regelung, die für Zwecke der Kriminalitätsbekämpfung *die Vorratsspeicherung* von Verkehrs- und Standortdaten vorsieht, … *allein die Bekämpfung der schweren Kriminalität eine solche Maßnahme zu rechtfertigen* (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 60 [wo die Formulierung „*im Hinblick auf das Ausmaß und die Schwere des Eingriffs*“ verwendet worden ist])“ (Hervorhebung nur hier). Rn. 115 des Urteils Tele2 greift diese Überlegung in Bezug auf den *Zugang* zu solchen Daten auf. Zur besonderen Schwere des betreffenden Eingriffs vgl. auch Rn. 97 und 100 dieses Urteils.

96 So wird in Rn. 115 des Urteils Tele2 betont, dass, „[*d*]*a außerdem der mit der [vom Grundsatz der Vertraulichkeit der elektronischen Kommunikation abweichenden nationalen] Regelung verfolgte Zweck im Verhältnis zur Schwere des mit dem Zugang einhergehenden Eingriffs* in die Grundrechte *stehen muss*, … folglich im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten *nur die Bekämpfung schwerer Straftaten einen solchen Zugang* zu den auf Vorrat gespeicherten Daten *zu rechtfertigen [vermag]*“ (Hervorhebung nur hier).

97 Dieses Gericht hat wiederholt die Notwendigkeit betont, einen *Ausgleich zwischen* dem Interesse eines Staates am Schutz seiner *nationalen Sicherheit* mit Hilfe von Maßnahmen, die personenbezogene Daten berühren, und der *Schwere der Verletzung* des Rechts einer Person auf Achtung ihres Privatlebens zu finden, zwei Faktoren, von denen der Ermessensspielraum des Staates abhängt, insbesondere wenn dieser *schwere Straftaten* verhindern oder verfolgen will (vgl. EGMR, 26. März 1987, Leander gegen Schweden, CE:ECHR:1987:0326JUD000924881, § 59; EGMR, 26. Juni 2006, Weber und Saravia gegen Deutschland, CE:ECHR:2006:0629DEC005493400, §§ 106, 125 und 126, sowie EGMR, 4. Dezember 2015, Roman Zakharov gegen Russland, CE:ECHR:2015:1204JUD004714306, §§ 232 und 244).

98 Siehe Nrn. 32 ff. dieser Schlussanträge.

Ermittlung zu Daten gerichtet ist, die von Dienstleistern für wirtschaftliche Zwecke gespeichert werden, und die ausschließlich die Identität (Name, Vorname und eventuell die Anschrift) einer begrenzten Gruppe von Teilnehmern oder Nutzern eines bestimmten Kommunikationsmittels betrifft, nämlich jene, deren Telefonnummer mit dem Mobiltelefon, dessen Diebstahl Gegenstand der Ermittlungen ist, in einem begrenzten Zeitraum, nämlich etwa zwölf Tagen, aktiviert worden ist [99].

85. Ich füge hinzu, dass die möglichen schädlichen Folgen für die von dem fraglichen Antrag auf Zugang Betroffenen sowohl moderat als auch begrenzt sind. Da die geforderten Daten ausschließlich in dem speziellen Rahmen einer Ermittlungsmaßnahme verwendet werden sollen, sind sie nicht für eine Verbreitung in der Öffentlichkeit bestimmt [100]. Darüber hinaus ist die den Polizeibehörden eingeräumte Zugangsmöglichkeit im spanischen Recht von Verfahrensgarantien eingehegt, denn sie unterliegt einer richterlichen Kontrolle, die übrigens im Ausgangsrechtsstreit zur Zurückweisung des Antrags der Polizei geführt hat.

86. Der sich aus der Übermittlung dieser Daten über die Identität ergebende Eingriff in die genannten Grundrechte ist meines Erachtens nicht besonders schwer [101], weil Daten einer solchen Art und einer so beschränkten Reichweite es für sich genommen nicht erlauben, verschiedene und/oder präzise Auskünfte über die betroffenen Personen zu erlangen [102], und deshalb die Intimität ihres Privatlebens unter diesen besonderen Umständen nicht unmittelbar und stark beeinträchtigen [103].

87. *Deshalb* bin ich, der Kommission folgend, der Meinung, dass, um dem vorlegenden Gericht sachdienliche Hinweise für die Entscheidung des ihm vorliegenden Rechtsstreits zu geben, die erste Vorlagefrage in der Weise *neuzufassen* ist, dass die vom Gerichtshof zu erwartende Antwort die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 im Hinblick auf Umstände wie diejenigen im vorliegenden Fall betrifft, nämlich einen Eingriff in die genannten Grundrechte, der nicht besonders schwer ist und der auf die Bekämpfung einer Art von Straftaten gerichtet ist, deren Schwere fraglich ist.

88. Insoweit erinnere ich daran, dass, da die Ziele, die eine nationale Regelung, die vom Grundsatz der Vertraulichkeit elektronischer Kommunikation abweicht, rechtfertigen, abschließend in Art. 15 Abs. 1 der Richtlinie 2002/58 aufgeführt sind, der Zugang zu den gespeicherten Daten tatsächlich und strikt einem dieser Ziele entsprechen muss [104]. Zu diesen Zielen gehört das Allgemeininteresse, „die Verhütung, Ermittlung, Feststellung und Verfolgung von *Straftaten*“ zu gewährleisten [105], ohne deren Art näher zu bezeichnen.

99 Ich weise darauf hin, dass der Gerichtshof in seinem Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017 (EU:C:2017:592, insbesondere Rn. 194 und 207 bis 209) auch die Notwendigkeit der Eingriffe durch das geplante Abkommen bewertet hat, indem er die darin geregelten Modalitäten der Datennutzung und -speicherung speziell unter dem Gesichtspunkt des besonderen Zusammenhangs dieser Maßnahmen, ihrer Bezeichnung und ihrer Dauer geprüft hat.

100 Wie dies beispielsweise bei der Identität von Personen, die in einem Pressebeitrag oder auf einer Internetseite veröffentlicht wird, der Fall sein könnte.

101 Vgl. in diesem Sinne das unter der Ägide des Europarats in Budapest am 23. November 2001 geschlossene und von allen Mitgliedstaaten der Union unterzeichnete Übereinkommen über Computerkriminalität (abrufbar unter der folgenden Internetadresse: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?_coeconventions_WAR_coeconventionsportlet_languageId=fr_FR), dessen Art. 18 vorschreibt, dass die gesetzgeberischen Maßnahmen getroffen werden, um die zuständigen Behörden zu ermächtigen, anzuordnen, dass ein Diensteanbieter Daten über Teilnehmer seiner Dienste, wie „die Identität …, seine Post[anschrift oder] Telefon[nummer]“, die sich in seinem Besitz befinden, vorzulegen hat.

102 Die dänische Regierung hat zu Recht darauf hingewiesen, dass wenn die Polizei, wie im vorliegenden Fall, Auskünfte über den Namen und die Anschrift des Eigentümers einer im Rahmen einer Straftat verwendeten SIM-Karte erhält, sich dies nicht grundlegend z. B. vom Erhalt von Informationen über den Eigentümer eines Fahrzeugs, das für die Begehung einer Straftat verwendet worden ist, unterscheidet.

103 Anders als besonders tief gehende Informationen insbesondere in Bezug auf die Nachverfolgbarkeit der Kommunikation und das Profil der betroffenen Personen, die Gegenstand der Rechtssachen waren, die zum Urteil Digital Rights (vgl. Rn. 26 bis 29 und 37) und zum Urteil Tele2 (vgl. Rn. 97 bis 100) geführt haben.

104 Vgl. insbesondere Rn. 90 und 115 des Urteils Tele2.

105 Hervorhebung nur hier.

89. Aus der verwendeten Terminologie ergibt sich, dass die Straftaten, die die betreffende einschränkende Maßnahme rechtfertigen, gemäß Art. 15 Abs. 1 nicht zwingend als „schwer" im Sinne der aus den Urteilen Digital Rights und Tele2 hervorgegangenen Rechtsprechung zu qualifizieren sein müssen. Meines Erachtens müssen nur dann, wenn der erlittene Eingriff, wie in den Rechtssachen, die zu den genannten Urteilen geführt haben, besonders schwer ist, auch die Straftaten, die einen solchen Eingriff rechtfertigen, besonders schwer sein. Im Fall eines nicht schweren Eingriffs ist dagegen zum Grundsatz zurückzukehren, der sich aus dem Wortlaut der Vorschrift ergibt, dass nämlich jede „Straftat" geeignet ist, einen solchen Eingriff zu rechtfertigen.

90. Meines Erachtens sollte darauf geachtet werden, die vom Gerichtshof in diesen beiden Urteilen aufgestellten Anforderungen nicht zu weit auszudehnen, um die den Mitgliedstaaten durch Art. 15 Abs. 1 eingeräumte Möglichkeit, von der Regelung der Richtlinie 2002/58 abzuweichen, in Fällen, in denen die betreffenden Eingriffe in das Privatleben zugleich ein legitimes Ziel verfolgen und eine begrenzte Reichweite haben, so wie jene, die im vorliegenden Fall die Folge des Antrags der Kriminalpolizei sein könnten, nicht oder zumindest nicht übermäßig zu beschränken. Konkret bin ich der Meinung, dass das Unionsrecht dem Zugang der zuständigen Behörden zu Identifikationsdaten im Besitz von Anbietern von Kommunikationsdiensten, die es gestatten, die möglichen Täter einer Straftat, die nicht schwer ist, aufzufinden, nicht entgegensteht.

91. Deshalb empfehle ich dem Gerichtshof, *auf die neu formulierte Vorlagefrage zu antworten*, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 sowie des Art. 52 Abs. 1 der Charta in der Weise auszulegen ist, dass eine Maßnahme, die den zuständigen nationalen Behörden für Zwecke der Bekämpfung von Straftaten unter Umständen wie jenen des Ausgangsverfahrens Zugang zu Daten über die Identität von Nutzern von Telefonnummern, die mit einem bestimmten Mobiltelefon in einem begrenzten Zeitraum aktiviert worden sind, gewährt, einen Eingriff in die von dieser Richtlinie und der Charta gewährleisteten Grundrechte darstellt, der keinen ausreichenden Schweregrad erreicht, um einen solchen Zugang auf Fälle zu beschränken, in denen die betreffende Straftat schwer ist.

92. In Anbetracht der vorgeschlagenen Antwort werden sämtliche noch folgenden Ausführungen nur hilfsweise und der Vollständigkeit halber gemacht.

2. Zur möglichen Bestimmung der für die Bestimmung der ausreichenden Schwere einer Straftat relevanten Kriterien

93. Für den Fall, dass der Gerichtshof entgegen meiner Empfehlung entscheiden sollte, dass in der vorliegenden Rechtssache trotz der besonderen Umstände des Ausgangsverfahrens zu bestimmen ist, was unter einer „schweren Straftat" im Sinne der aus den Urteilen Digital Rights und Tele2 hervorgegangenen Rechtsprechung zu verstehen ist[106], ist *erstens* noch zu klären, ob es sich bei dieser Bewertung um einen *autonomen Begriff* des Unionsrechts handelt, der somit vom Gerichtshof zu definieren ist. Der von der französischen Regierung in der Hauptsache vorgeschlagenen Antwort folgend ist das jedoch nicht meine Überzeugung, und zwar aus den folgenden Gründen.

106 Wenn also der Gerichtshof annähme, dass der Eingriff im Ausgangsverfahren ausreichend schwer ist, damit die erste Frage so beantwortet wird, wie sie vom vorlegenden Gericht gestellt worden ist, oder dass es insoweit unerheblich ist, dass dieser Eingriff nicht schwer ist.

94. Zunächst stelle ich fest, dass die Richtlinie 2006/24, aus der sich die Verwendung des Begriffs der „schweren Straftat“ ergibt [107], diesen Begriff nicht definiert, sondern insoweit auf die Rechtsordnungen der Mitgliedstaaten verweist [108]. Außerdem bin ich der Meinung, dass die zutreffenden Erwägungen in den Urteilen Digital Rights und Tele2 nicht so zu verstehen sind, dass sie eine Harmonisierung der in den Mitgliedstaaten geltenden Rechtsvorschriften zum Inhalt dieses Begriffs anstreben.

95. Insoweit erinnere ich daran, dass die Strafgesetzgebung und das Strafverfahren in die Zuständigkeit der Mitgliedstaaten fallen, auch wenn ihr Recht von Bestimmungen des Unionsrechts in diesem Bereich berührt werden kann [109]. Nach dem Wortlaut von Art. 83 Abs. 2 AEUV können nur, wenn sich die Angleichung der strafrechtlichen Rechtsvorschriften der Mitgliedstaaten für die wirksame Durchführung der Politik der Union auf einem Gebiet, auf dem Harmonisierungsmaßnahmen erfolgt sind, als unerlässlich erweist, durch Richtlinien Mindestvorschriften für die Festlegung von Straftaten und Strafen auf dem betreffenden Gebiet festgelegt werden. Nach dem gegenwärtigen Stand des Unionsrechts gibt es jedoch keine allgemeine Bestimmung, die den Begriff der „schweren Straftat“ definiert [110].

96. Die Befugnis zu definieren, was eine „schwere Straftat“ ist, liegt grundsätzlich bei den zuständigen Stellen der Mitgliedstaaten. Der Gerichtshof hat jedoch aufgrund der Vorabentscheidungsersuchen, mit denen die Mitgliedstaaten ihn befassen können, die Aufgabe, über die Einhaltungen aller Anforderungen des Unionsrechts zu wachen und insbesondere eine kohärente Anwendung des durch die Bestimmungen der Charta gewährten Schutzes sicherzustellen.

97. Die betreffende rechtliche Einordnung kann nicht nur von einem Mitgliedstaat zum anderen je nach seinen Traditionen und Prioritäten variieren, sondern auch im Laufe der Zeit unter dem Einfluss der Strafrechtspolitik in Richtung einer größeren oder geringeren Strenge, um der Entwicklung der Kriminalität Rechnung zu tragen [111], sowie allgemeiner den gesellschaftlichen Veränderungen und den nationalen Bedürfnissen insbesondere hinsichtlich der Strafverfolgung.

98. Außerdem weise ich darauf hin, dass sich angesichts der großen Unterschiede zwischen den traditionell in verschiedenen Mitgliedstaaten geltenden Strafmaßen [112] die Schwere einer Straftat nicht ausschließlich aus der Schwere der Strafe, mit der sie belegt ist, ergibt. Die Frage, ob eine Straftat schwer ist, ist insofern sehr relativ, als sie von der Skala der Strafen abhängt, die im Allgemeinen in dem betreffenden Mitgliedstaat verhängt werden. So kann von der Tatsache, dass ein Mitgliedstaat eine niedrige Freiheitstrafe oder sogar eine Alternative zur Freiheitsstrafe vorsieht, nicht auf die intrinsische Schwere der betreffenden Straftat geschlossen werden [113].

107 Siehe Nr. 71 dieser Schlussanträge.

108 Art. 1 Abs. 1 der Richtlinie 2006/24 bestimmte, dass mit dieser Richtlinie „die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste … harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung *von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen*“ (Hervorhebung nur hier). Vgl. auch den 21. Erwägungsgrund dieser Richtlinie.

109 Vgl. insbesondere Urteile vom 15. September 2011, Dickinger und Ömer (C-347/09, EU:C:2011:582, Rn. 31), sowie vom 6. Dezember 2011, Achughbabian (C-329/11, EU:C:2011:807, Rn. 33).

110 Siehe hierzu auch Nr. 112 dieser Schlussanträge.

111 Zur Dynamik der schweren Kriminalität vgl. insbesondere meine Schlussanträge in den verbundenen Rechtssachen Tele2 Sverige u. a. (C-203/15 und C-698/15, EU:C:2016:572, Nr. 214).

112 So gibt im Bereich der Bekämpfung der organisierten Kriminalität ein Bericht der Kommission vom 7. Juli 2016 an, dass die in den Mitgliedstaaten vorgesehenen Strafen für die schwere Straftat der Beteiligung an einer kriminellen Vereinigung von einem Mitgliedstaat zum anderen erheblich variieren (zwischen drei Monaten und 17 Jahren Gefängnis) (vgl. Bericht der Kommission an das Europäische Parlament und den Rat gemäß Artikel 10 des Rahmenbeschlusses 2008/841/JI vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität, COM[2016] 448 final, S. 7, Punkt 2.1.4.1).

113 Wie die Regierung Dänemarks erklärt hat, gelten in Dänemark im Vergleich zu anderen Mitgliedstaaten weniger schwere Strafen, ohne dass dies bedeuten würde, dass die Straftat als nicht besonders schwer angesehen wird. So beträgt z. B. die Strafe für den Besitz von kinderpornografischem Material ein Jahr Freiheitsstrafe, während sie für die gleiche Tat in anderen Mitgliedstaaten bis zu zehn Jahre Freiheitsstrafe betragen könnte. Dies stellt jedoch die Feststellung nicht in Frage, dass diese Straftat ihrer Art nach besonders schwer ist.

99. Meines Erachtens sind, analog zur Rechtsprechung des Gerichtshofs zum Schutz der öffentlichen Sicherheit [114], einem meines Erachtens insbesondere in Anbetracht des Wortlauts von Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 mit dem Begriff der Bekämpfung der schweren Kriminalität verwandten Begriff, die Besonderheiten der Strafrechtsordnungen der Mitgliedstaaten zu respektieren, soweit das Unionsrecht den Mitgliedstaaten keine strikten Pflichten auferlegt.

100. Ich bin deshalb hilfsweise der Ansicht, dass der Begriff der „schweren Straftat" im Sinne der aus den Urteilen Digital Rights und Tele2 hervorgegangenen Rechtsprechung des Gerichtshofs keinen autonomen Begriff des Unionsrechts darstellt, dessen Inhalt vom Gerichtshof zu bestimmen wäre, auch wenn die in Art. 15 Abs. 1 der Richtlinie 2002/58 geregelte Ausnahme von den Mitgliedstaaten im Einklang mit den sich aus dem Unionsrecht, insbesondere aus den von der Charta gewährten Grundrechten, ergebenden Pflichten anzuwenden ist, und zwar unter der Kontrolle des Gerichtshofs.

101. Insoweit weise ich darauf hin, dass sich aus der Rechtsprechung des Gerichtshofs insbesondere ergibt, dass Art. 15 Abs. 1, soweit er es den Mitgliedstaaten gestattet, die Reichweite bestimmter in dieser Richtlinie vorgesehener Rechte und Pflichten zu beschränken, eng auszulegen ist und nicht dazu führen kann, dass die Ausnahme von diesen grundsätzlichen Rechten und Pflichten die Regel wird [115]. Die Reichweite des Begriffs der „schweren Straftat" kann also von den Mitgliedstaaten nicht übermäßig weit ausgedehnt werden.

102. *Zweitens* und höchst hilfsweise müsste der *Gerichtshof, wenn er annähme, dass der Begriff autonom ist*, auf die Frage, so wie sie vom vorlegenden Gericht formuliert ist, antworten und sich folglich zur Bestimmung der Kriterien äußern, die auf der Ebene des Unionsrechts die Beurteilung erlauben, ob eine Straftat ausreichend schwer ist, um einen Eingriff in die in den Art. 7 und 8 der Charta geregelten Grundrechte zu rechtfertigen.

103. Genauer müsste der Gerichtshof bestimmen, ob es für den Nachweis des Bestehens einer „schweren Straftat" im Sinne dieser Rechtsprechung ausreichend ist, sich auf die für die behauptete Straftat vorgesehene Strafe zu stützen, oder ob es darüber hinaus erforderlich ist, bei dem deliktischen Verhalten bestimmte Grade der Schädlichkeit für Individual- oder Kollektivrechtsgüter festzustellen. Insoweit sollte meines Erachtens sowie nach Ansicht der Regierungen Dänemarks, Spaniens, Frankreichs, Ungarns, Österreichs, Polens und des Vereinigten Königreichs die Wahl nicht auf die erste, sondern auf die zweite Alternative fallen, wobei einer auf eine *Mehrheit von Beurteilungskriterien* gestützten Definition der Vorzug zu geben ist [116].

104. Was die Schwere der Straftat betrifft, die einen Zugang zu den Daten rechtfertigen kann, wäre es meines Erachtens in Anbetracht des Verhältnismäßigkeitsprinzips unmöglich, die Schwere der vorgeworfenen Tat nur auf der Grundlage des Strafrahmens zu bestimmen. In Anbetracht der erheblichen Unterschiede, die noch zwischen den Strafrechtsordnungen der Mitgliedstaaten bestehen, bin ich der Meinung, dass nicht angenommen werden kann, dass das Strafmaß allein, sei es unter dem qualitativen Blickwinkel der Art der Strafe und/oder unter dem quantitativen Blickwinkel des Strafmaßes, die besondere Schwere einer Straftat widerspiegelt.

114 Vgl. insbesondere Urteil vom 22. Mai 2012, I (C-348/09, EU:C:2012:300, Rn. 21 bis 23), wonach „das Unionsrecht den Mitgliedstaaten keine einheitliche Werteskala für die Beurteilung von Verhaltensweisen vorschreibt, die als Verletzung der öffentlichen Sicherheit angesehen werden können" und dass „es den Mitgliedstaaten im Wesentlichen [zwar] weiterhin [freisteht], nach ihren nationalen Bedürfnissen, die je nach Mitgliedstaat und Zeitpunkt unterschiedlich sein können, zu bestimmen, was die öffentliche Ordnung und Sicherheit erfordern", dass aber „diese Anforderungen, insbesondere wenn sie eine Ausnahme von dem grundlegenden Prinzip der Freizügigkeit rechtfertigen sollen, eng zu verstehen [sind], so dass ihre Tragweite nicht von jedem Mitgliedstaat einseitig ohne Kontrolle durch die Organe der Europäischen Union bestimmt werden kann".

115 Vgl. in diesem Sinne Rn. 89 ff. des Urteils Tele2 in Bezug auf die grundsätzliche Pflicht, die Vertraulichkeit der Kommunikation und der auf sie bezogenen Verkehrsdaten zu gewährleisten.

116 Ich weise darauf hin, dass die Regierungen Tschechiens und Estlands vorschlagen, zu antworten, dass es möglich ist, die hinreichende Schwere der Straftaten als Kriterium, das einen Eingriff in die in den Art. 7 und 8 der Charta geregelten Grundrechte rechtfertigt, allein auf der Grundlage des Strafmaßes zu bestimmen, dass diese Regierungen jedoch der Meinung sind, dass jeder Mitgliedstaat frei bleiben sollte, andere objektive Kriterien, die der Besonderheit seiner Rechtsordnung Rechnung tragen, zu berücksichtigen, wenn er es für notwendig hält.

105. Auch wenn der Strafe eine beachtliche Bedeutung zukommt, müssen insoweit von Fall zu Fall andere objektive Faktoren ebenso berücksichtigt werden. Konkret handelt es sich zum einen um den Zusammenhang, in dem die behauptete Straftat steht – ob das deliktische Verhalten vorsätzlich begangen worden ist, ob erschwerende Umstände hinzukommen und/oder ob es sich um eine Wiederholungstat handelt –, und zum anderen um die Bedeutung der Interessen der Gesellschaft, die der Straftäter missachtet hat, sowie um die Art und/oder den Umfang der Schäden des Opfers der Straftat [117] und schließlich um die Skala der in dem betreffenden Mitgliedstaat im Allgemeinen anwendbaren Strafen [118]. Auf der Grundlage dieses Bündels von alternativen und nicht abschließenden Beurteilungskriterien ist meines Erachtens eine Straftat möglicherweise als „schwer" im Sinne der fraglichen Rechtsprechung des Gerichtshofs zu qualifizieren.

106. Die vorgeschlagene Auslegung entspricht außerdem dem vom EGMR in seiner Rechtsprechung zur „Prävention von Straftaten" gewählten Ansatz eines Ziels, das einen Eingriff in das in Art. 8 EMRK geregelte Recht auf Privatleben unter dem Vorbehalt rechtfertigt, dass auch noch weitere Voraussetzungen erfüllt sind [119]. Aus dieser Rechtsprechung ergibt sich meines Erachtens, dass sich die Vertragsstaaten der EMRK in diesem Rahmen auf die Bekämpfung bestimmter Kategorien von Straftaten berufen können [120], und zwar im Hinblick nicht so sehr nur auf das Strafmaß, sondern vielmehr auf verschiedene Faktoren, zu denen insbesondere auch die Art der betreffenden Straftat sowie die von ihr berührten öffentlichen und privaten Interessen gehören [121].

107. Ich bin deshalb der Meinung, dass wenn der Begriff der „schweren Straftat" im Sinne der aus den Urteilen Digital Rights und Tele2 hervorgegangenen Rechtsprechung vom Gerichtshof als autonomer Begriff des Unionsrechts angesehen würde, er in dem Sinne auszulegen wäre, dass die Schwere einer Straftat, die gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 den Zugang der zuständigen nationalen Behörden zu personenbezogenen Daten rechtfertigen könnte, nicht ausschließlich unter Berücksichtigung des Strafrahmens, sondern darüber hinaus unter Berücksichtigung einer Reihe von anderen objektiven Beurteilungskriterien wie den oben genannten beurteilt werden müsste.

D. Zur hilfsweisen Definition der Mindeststrafe, die erforderlich ist, um die ausreichende Schwere einer Straftat, die einen Eingriff in die genannten Grundrechte rechtfertigt, zu begründen (zweite Frage)

108. Mit seiner zweiten Frage möchte das vorlegende Gericht vom Gerichtshof wissen, wie hoch die Mindeststrafe sein muss, damit eine Straftat im Sinne der aus den Urteilen Digital Rights und Tele2 hervorgegangenen Rechtsprechung als „schwer" angesehen werden kann, und ob eine allgemeine Grenze von drei Jahren Freiheitsentzug, wie sie seit der Reform von 2015 in der spanischen Strafprozessordnung vorgesehen ist [122], mit den Anforderungen des Unionsrechts vereinbar ist.

117 Ich teile die Auffassung der französischen Regierung, nach der es sich von selbst versteht, dass Verletzungen der grundlegenden Interessen der Nation, der Institutionen oder der Unverletzlichkeit des Staatsgebiets ihrem Wesen nach der „schweren Kriminalität" zuzurechnen sind, dass aber auch andere Arten von Straftaten dazugezählt werden sollten, wie etwa Verletzungen des Lebens, der körperlichen oder psychischen Integrität und der Würde des Menschen sowie Verletzungen von Sachen, die einen erheblichen Vermögensschaden des Opfers zur Folge haben oder solche, die in Serie begangen werden und die öffentliche Ordnung wiederholt verletzen. Zu diesem letzten Punkt nennt die ungarische Regierung auch die Möglichkeit, eine außergewöhnliche Häufung bestimmter Straftaten in der nationalen Kriminalität zu berücksichtigen.

118 Vgl. hierzu auch oben Nr. 98 dieser Schlussanträge.

119 Gemäß Art. 8 Abs. 2 EMRK ist ein solcher Eingriff nur gerechtfertigt, soweit er gesetzlich vorgesehen, auf eines der in diesem Absatz genannten Ziele gerichtet und in einer demokratischen Gesellschaft notwendig ist, um dieses Ziel bzw. diese Ziele zu erreichen.

120 Der Gerichtshof hat entschieden, dass es den Bürgern möglich sein muss, die einschlägigen Straftaten leicht zu bestimmen, ohne dass dieses Erfordernis der Voraussehbarkeit voraussetzt, dass die Staaten die Straftaten, die eine solche Maßnahme zur Folge haben können, abschließend aufzählen (vgl. insbesondere EGMR, 4. Dezember 2015, Roman Zakharov gegen Russland, CE:ECHR:2015:1204JUD004714306, § 244).

121 Vgl. insbesondere EGMR, 26. Juni 2006, Weber und Saravia gegen Deutschland (CE:ECHR:2006:0629DEC005493400, §§ 106 und 115); EGMR, 4. Dezember 2008, Marper gegen Vereinigtes Königreich (CE:ECHR:2008:1204JUD003056204, §§ 104 und 119), sowie EGMR, 30. Mai 2017, Trabajo Rueda gegen Spanien (CE:ECHR:2017:0530JUD003260012, §§ 39 und 40).

122 Siehe Nrn. 15 ff. dieser Schlussanträge.

109. Diese Fragen werden nur hilfsweise für den Fall gestellt, dass der Gerichtshof bei der Beantwortung der ersten Vorlagefrage entscheiden sollte, dass die Schwere einer Straftat, die nach der genannten Rechtsprechung einen Eingriff in Grundrechte rechtfertigen kann, ausschließlich unter Berücksichtigung des Strafmaßes der Freiheitsstrafe, die verhängt werden kann, zu beurteilen ist.

110. In Anbetracht der Antwort, die ich in Bezug auf die erste Frage vorschlage, hat der Gerichtshof meines Erachtens über die zweite Frage nicht zu entscheiden. Gleichwohl nehme ich der Vollständigkeit halber hierzu Stellung.

111. Was den *ersten Teil der zweiten Frage* betrifft, bin ich, den Regierungen Tschechiens und Estlands folgend, der Meinung, dass das *Strafmaß*, aufgrund dessen allein eine Straftat als „schwer" zu qualifizieren wäre, in Anbetracht der vorstehenden Erwägungen im Rahmen der Beantwortung der ersten vom vorlegenden Gericht gestellten Frage nicht für das gesamte Gebiet der Union einheitlich bestimmt werden kann [123].

112. Diese Variation in der Definition der „schweren Straftat" und insbesondere hinsichtlich der Mindeststrafe, die erreicht sein muss, damit eine Straftat als schwer angesehen werden kann, findet sich übrigens auch in den Rechtsakten der Union wieder. Auf der Grundlage von Art. 83 Abs. 1 AEUV erlassene Unionsrechtsakte sehen Freiheitsstrafen unterschiedlicher Höhe für Straftaten vor, die freilich sämtlich einer „besonders schweren Kriminalität" zugerechnet werden [124], wie sich beispielsweise aus Art. 3 der Richtlinie 2011/92/EU [125] und aus Art. 15 der Richtlinie (EU) 2017/541 [126] ergibt, die die Bekämpfung des sexuellen Missbrauchs Minderjähriger bzw. die Bekämpfung des Terrorismus betreffen.

113. Ich erinnere daran, dass die Freiheit der Mitgliedstaaten, über das Mindeststrafmaß zu entscheiden, das erforderlich ist, damit Straftaten als „schwer" bezeichnet werden können, durch Vorschriften in den Bestimmungen des Unionsrechts in diesem Bereich, aber auch durch den Grundsatz, nach dem einer Ausnahme keine so große Reichweite gegeben werden kann, dass sie faktisch zur allgemeinen Regel würde, begrenzt wird [127].

114. Auch wenn im vorliegenden Fall jeder Mitgliedstaat in der Beurteilung, was ein für eine schwere Straftat angemessenes Strafmaß ist, frei ist, ist er gleichwohl verpflichtet, dieses nicht auf ein im Verhältnis zu den in diesem Staat üblichen Strafen derart niedriges Maß festzulegen [128], dass die in diesem Art. 15 Abs. 1 vorgesehenen Ausnahmen vom Verbot der Speicherung und Nutzung zur Regel gemacht werden, wie die Regierung Irlands zu Recht angemerkt hat.

115. Darüber hinaus steht fest, dass die Eingriffe in die durch die Art. 7 und 8 der Charta gewährleisteten Grundrechte, die den Mitgliedstaaten gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 gestattet sein können, stets die allgemeinen Anforderungen des Verhältnismäßigkeitsgrundsatzes, so wie er sich aus Art. 52 Abs. 1 der Charta ergibt, beachten müssen [129].

123 Siehe Nrn. 93 ff. dieser Schlussanträge.

124 Art. 83 Abs. 1 AEUV gestattet die Festlegung von „Mindestvorschriften zur Festlegung von Straftaten und Strafen in [in dieser Vorschrift genannten] Bereichen besonders schwerer Kriminalität …, die … eine grenzüberschreitende Dimension haben".

125 Richtlinie 2011/92/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. 2011, L 335, S. 1), deren Art. 3 für verschiedene Arten von „Straftaten im Zusammenhang mit sexuellem Missbrauch" Mindestfreiheitsstrafen von einem bis zu zehn Jahren vorsieht.

126 Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates (ABl. 2017, L 88, S. 6), deren Art. 15 Abs. 3 für die verschiedenen in Art. 4 der Richtlinie genannten „Straftaten im Zusammenhang mit einer terroristischen Vereinigung" Freiheitsstrafen von mindestens acht oder fünfzehn Jahren vorsieht.

127 Siehe auch Nr. 101 dieser Schlussanträge.

128 Siehe hierzu Nr. 98 dieser Schlussanträge.

129 Vgl. insbesondere den elften Erwägungsgrund und Art. 15 Abs. 1 der Richtlinie 2002/58 sowie die Rn. 94 bis 96 und 116 des Urteils Tele2.

116. Was den *letzten Teil der zweiten Frage* anbelangt, weisen die Regierung Estlands und die Kommission darauf hin, dass eine Schwelle, die ausschließlich auf einer Mindeststrafe von drei Jahren Freiheitsstrafe beruht, absolut betrachtet ausreichend ist, um eine Straftat als „schwer" im Sinne der aus dem Urteil Digital Rights hervorgegangenen Rechtsprechung des Gerichtshofs zum Zugang zu personenbezogenen Daten anzusehen, und dass eine solche Schwelle nicht mit dem Unionsrecht im Allgemeinen [130] und Art. 15 Abs. 1 der Richtlinie 2002/58 im Besonderen offensichtlich unvereinbar ist.

117. Es wäre jedoch meines Erachtens wünschenswert, dass der Gerichtshof darauf verzichtet, sich für ein bestimmtes Strafmaß auszusprechen, weil das, was für manche Mitgliedstaaten angemessen ist, für andere nicht notwendig angemessen sein wird und das, was heute für eine bestimmte Art von Straftat gilt, nicht notwendig unwiderruflich für die Zukunft gilt, wie ich bereits erklärt habe [131]. Wenn die Bestimmung der betreffenden Schwelle eine komplexe und potenziell einer Entwicklung unterworfene Bewertung erfordert, ist insoweit meines Erachtens Vorsicht geboten und sollte diese Bestimmung im Rahmen der ihm übertragenen Zuständigkeiten der Beurteilung durch den Unionsgesetzgeber oder, in den Grenzen der sich aus dem Unionsrecht ergebenden Anforderungen, der Beurteilung eines jeden Mitgliedstaats überlassen werden.

118. Insoweit stelle ich fest, dass vorliegend das vorlegende Gericht auf die, oben bereits erwähnte [132], Gefahr einer Umkehrung des Grundsatzes und der in der Richtlinie 2002/58 vorgesehenen Ausnahmen hinweist, indem es erklärt, dass „[d]ie Bezugnahme auf die Strafe – wobei der [vom spanischen Gesetzgeber 2015 eingeführte [133]] Strafrahmen mindestens drei Jahre Freiheitsentzug erreichen muss – … eine deutliche Mehrheit der Straftypen [umfasst]". Die aktuelle, durch die Reform der Strafprozessordnung eingeführte Liste der Straftaten, die in Spanien Beschränkungen der gemäß den Art. 7 und 8 der Charta geschützten Rechte rechtfertigen können, würde mit anderen Worten nach diesem Gericht dazu führen, dass die Mehrheit der im Strafgesetzbuch geregelten Straftaten Bestandteil dieser Liste wäre.

119. Würde jedoch der Gerichtshof den Eingriff im Ausgangsverfahren als schwer ansehen und träte das vom vorlegenden Gericht genannte Ergebnis ein, wäre dieses meines Erachtens mit dem Erfordernis der Verhältnismäßigkeit, dem solche Einschränkungen unterliegen, nicht vereinbar [134]. Das gilt meines Erachtens trotz des von der spanischen Regierung geltend gemachten Vorhandenseins einer gerichtlichen Kontrolle, weil die Ausübung dieser Kontrolle es nur erlaubt, die Umsetzung von Maßnahmen, die im Einzelfall als willkürlich oder zu stark eingreifend angesehen werden, zu verhindern, nicht aber, den Rückgriff auf solche Maßnahmen und deren Entwicklung grundsätzlich zu bremsen.

120. Schließlich weise ich darauf hin, dass die in diesem Abschnitt vorgeschlagene Herangehensweise mit derjenigen des EGMR in seiner Rechtsprechung zum Schutz personenbezogener Daten übereinstimmt. Zwar hat dieses Gericht, wie die Regierung Irlands und die Kommission vortragen, die nationalen Rechte, die die „schweren" Straftaten, die einen Eingriff in das Privatleben rechtfertigen können, unter Bezugnahme auf ein Strafmaß von mindestens drei Jahren Freiheitsstrafe definieren, für ausreichend klar gehalten [135]. Gleichwohl bin ich der Meinung, dass es dieses Strafmaß für die Zwecke

130 Vgl. insbesondere, neben den in den Fn. 125 und 126 dieser Schlussanträge genannten Vorschriften, die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (ABl. 2016, L 119, S. 132), deren Art. 3 Nr. 9 „schwere Kriminalität" als „die in Anhang II aufgeführten strafbaren Handlungen, die nach dem nationalen Recht eines Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind", definiert.

131 Siehe Nr. 97 dieser Schlussanträge.

132 Siehe Nr. 101 dieser Schlussanträge.

133 In den Nrn. 15 ff. der vorliegenden Schlussanträge erwähnte Reform.

134 Siehe auch Nr. 115 dieser Schlussanträge.

135 Vgl. in diesem Sinne EGMR, 18. Mai 2010, Kennedy gegen Vereinigtes Königreich (ECLI:CE:ECHR:2010:0518JUD002683905, §§ 34 und 159), sowie EGMR, 4. Dezember 2015, Roman Zakharov gegen Russland (CE:ECHR:2015:1204JUD004714306, § 244).

dieser Definition nicht zu einem absoluten und unveränderlichen Kriterium erhoben hat, zumal mir seine Rechtsprechung auf das Erfordernis einer Voraussehbarkeit und ausreichenden Klarheit für die Bürger nicht so sehr in Bezug auf das Strafmaß, als vielmehr auf die Art der Straftat, die einen solchen Eingriff zulässt, fokussiert zu sein scheint [136]. Auch wenn der EGMR im Übrigen den Staaten einen Spielraum bei der Beurteilung des Bestehens und der Reichweite der Notwendigkeit eines solchen Eingriffs einräumt, unterwirft er diesen Ermessensspielraum gleichwohl einer Kontrolle auf europäischer Ebene [137]. Insbesondere achtet er auf die Vermeidung der Gefahr von Missbrauch, die durch Gesetze hervorgerufen wird, die einen so weiten Strauß an Straftaten vorsehen, dass sie dazu führen, dass die meisten Straftaten eingreifende Maßnahmen rechtfertigen können [138].

121. Zusammengefasst bin ich deshalb der Meinung, dass für den Fall, dass der Gerichtshof – entgegen meiner Empfehlung – entscheiden sollte, dass für die Einordnung einer Straftat als „schwer" im Sinne der aus dem Urteil Digital Rights hervorgegangenen Rechtsprechung nur das Strafmaß zu berücksichtigen ist, auf die zweite Vorlagefrage zu antworten wäre, dass die Mitgliedstaaten bei der Bestimmung der Mindesthöhe der hierfür maßgeblichen Strafe frei sind, soweit sie die Anforderungen des Unionsrechts und insbesondere jene, nach denen die Eingriffe in die in den Art. 7 und 8 der Charta gewährleisteten Grundrechte die Ausnahme bleiben und den Verhältnismäßigkeitsgrundsatz beachten müssen, beachten.

V. Ergebnis

122. Nach alledem schlage ich dem Gerichtshof vor, auf die Vorlagefragen der Audiencia Provincial de Tarragona (Regionalgericht Tarragona, Spanien) wie folgt zu antworten:

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 seiner 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 sowie des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union in der Weise auszulegen, dass eine Maßnahme, die den zuständigen nationalen Behörden für die Zwecke der Bekämpfung von Straftaten Zugang unter Umständen wie denjenigen des Ausgangsverfahrens zu Informationsdaten der Nutzer der mit einem bestimmten Mobiltelefon in einem begrenzten Zeitraum aktivierten Telefonnummern gewährt, einen Eingriff in die durch diese Richtlinie und die Charta gewährleisteten Grundrechte zur Folge hat, der keinen ausreichenden Schweregrad erreicht, um einen solchen Zugang auf Fälle zu beschränken, in denen die betreffende Straftat als schwer anzusehen ist.

136 Siehe Nr. 106 dieser Schlussanträge.

137 Vgl. insbesondere EGMR, 6. September 1978, Klass u. a. gegen Deutschland (CE:ECHR:1978:0906JUD000502971, § 49), sowie EGMR, 18. Mai 2010, Kennedy gegen Vereinigtes Königreich (CE:ECHR:2010:0518JUD002683905, §§ 153 und 154).

138 Vgl. EGMR, 10. Februar 2009, Iordachi u. a. gegen Moldawien (CE:ECHR:2009:0210JUD002519802, § 44), in dem angenommen wurde, dass das moldawische Recht nicht ausreichend klar sei, weil mehr als die Hälfte der im Strafgesetzbuch geregelten Straftaten in die Kategorie der Straftaten fiel, die zu einer Maßnahme der Telefonabhörung führen können. Vgl. auch EGMR, 4. Dezember 2015, Roman Zakharov gegen Russland (CE:ECHR:2015:1204JUD004714306, § 248).