

Quelle: <http://curia.europa.eu/>

URTEIL DES GERICHTSHOFS (Große Kammer)

30. April 2024(*)

„Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation – Vertraulichkeit der Kommunikation – Betreiber elektronischer Kommunikationsdienste – Richtlinie 2002/58/EG – Art. 15 Abs. 1 – Art. 7, 8 und 11 sowie Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union – Von einer zuständigen nationalen Behörde zur Strafverfolgung von schweren Diebstählen beantragter Zugang zu diesen Daten – Definition des Begriffs ‚schwere Straftat‘, deren Verfolgung einen schweren Eingriff in Grundrechte rechtfertigen kann – Zuständigkeit der Mitgliedstaaten – Grundsatz der Verhältnismäßigkeit – Umfang der vorherigen gerichtlichen Kontrolle von Anträgen auf Zugang zu von Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten“

In der Rechtssache C-178/22

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Giudice delle indagini preliminari presso il Tribunale di Bolzano (Ermittlungsrichter beim Landesgericht Bozen, Italien) mit Entscheidung vom 20. Februar 2022, beim Gerichtshof eingegangen am 8. März 2022, in den Strafverfahren gegen

Unbekannt,

Beteiligte:

Procura della Repubblica presso il Tribunale di Bolzano,

erlässt

DER GERICHTSHOF (Große Kammer)

unter Mitwirkung des Präsidenten K. Lenaerts, des Vizepräsidenten L. Bay Larsen, des Kammerpräsidenten A. Arabadjiev, der Kammerpräsidentinnen A. Prechal und K. Jürimäe, der Kammerpräsidenten T. von Danwitz und Z. Csehi, der Richter J.-C. Bonichot, S. Rodin, P. G. Xuereb (Berichterstatter) und D. Gratsias sowie der Richterin M. L. Arastey Sahún und des Richters M. Gavalec,

Generalanwalt: A. M. Collins,

Kanzler: C. Di Bella, Verwaltungsrat,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 21. März 2023,

unter Berücksichtigung der Erklärungen

- der Procura della Repubblica presso il Tribunale di Bolzano, vertreten durch F. Iovene, Sostituto procuratore della Repubblica,
- der italienischen Regierung, vertreten durch G. Palmieri als Bevollmächtigte im Beistand von S. Faraci, Avvocato dello Stato,
- der tschechischen Regierung, vertreten durch A. Edelmannová, O. Serdula, M. Smolek, T. Suchá und J. Vlácil als Bevollmächtigte,
- der estnischen Regierung, vertreten durch M. Kriisa als Bevollmächtigte,
- Irlands, vertreten durch M. Browne, Chief State Solicitor, A. Joyce und M. Tierney als Bevollmächtigte im Beistand von D. Fennelly, BL,
- der französischen Regierung, vertreten durch A. Daniel, A.-L. Desjonquères, B. Fodda und J. Illouz als Bevollmächtigte,
- der zyprischen Regierung, vertreten durch E. Neophytou als Bevollmächtigte,
- der ungarischen Regierung, vertreten durch Zs. Biró-Tóth und M. Z. Fehér als Bevollmächtigte,
- der niederländischen Regierung, vertreten durch K. Bulterman, A. Hanje und J. Langer als Bevollmächtigte,
- der österreichischen Regierung, vertreten durch A. Posch, J. Schmoll, C. Gabauer, K. Ibili und E. Samoiloვა als Bevollmächtigte,
- der polnischen Regierung, vertreten durch B. Majczyna, D. Lutostańska und J. Sawicka als Bevollmächtigte,
- der Europäischen Kommission, vertreten durch S. L. Kalèda, H. Kranenborg, L. Malferrari und F. Wilman als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 8. Juni 2023

folgendes

Urteil

- 1 Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung (im Folgenden: Richtlinie 2002/58) im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).
- 2 Dieses Ersuchen ergeht im Rahmen einer Anrufung des Giudice delle indagini preliminari presso il Tribunale di Bolzano (Ermittlungsrichter beim Landesgericht Bozen, Italien) durch die Procura della Repubblica presso il Tribunale di Bolzano (Staatsanwaltschaft beim Landesgericht Bozen, Italien) (im Folgenden: Staatsanwaltschaft), um von ihm zur Ermittlung der Täter zweier schwerer Diebstähle von Mobiltelefonen die Genehmigung für den Zugang zu personenbezogenen Daten zu erhalten, die von Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert wurden.

Rechtlicher Rahmen

Unionsrecht

Richtlinie 2002/58

- 3 In den Erwägungsgründen 2 und 11 der Richtlinie 2002/58 heißt es:
„(2) Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die Charta ... anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 [der] Charta niedergelegten Rechte uneingeschränkt geachtet werden.

...

(11) Wie die Richtlinie 95/46/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)] 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 [am 4. November 1950 in Rom unterzeichneten] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein sowie angemessenen Garantien gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten entsprechen.“

4 Art. 2 („Begriffsbestimmungen“) der Richtlinie 2002/58 bestimmt:

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

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

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

...“

- 5 Art. 5 („Vertraulichkeit der Kommunikation“) der Richtlinie 2002/58 sieht vor:

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

...

(3) Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie [95/46] u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.“

- 6 Art. 6 („Verkehrsdaten“) der Richtlinie 2002/58 bestimmt:

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

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

(3) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann die in Absatz 1 genannten Daten zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu oder zur Vermarktung erforderlichen Zeitraums verarbeiten, sofern der Teilnehmer oder der Nutzer, auf den sich die Daten beziehen, zuvor seine Einwilligung gegeben hat. Der Nutzer oder der Teilnehmer hat die Möglichkeit, seine Einwilligung zur Verarbeitung der Verkehrsdaten jederzeit zu widerrufen.

...

(5) Die Verarbeitung von Verkehrsdaten gemäß den Absätzen 1, 2, 3 und 4 darf nur durch Personen erfolgen, die auf Weisung der Betreiber öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste handeln und die für Gebührenabrechnungen oder Verkehrsabwicklung, Kundenanfragen, Betrugsermittlung, die Vermarktung der elektronischen Kommunikationsdienste oder für die Bereitstellung eines Dienstes mit Zusatznutzen zuständig sind; ferner ist sie auf das für diese Tätigkeiten erforderliche Maß zu beschränken.

...“

7 Art. 9 („Andere Standortdaten als Verkehrsdaten“) Abs. 1 der Richtlinie 2002/58 sieht vor:

„Können andere Standortdaten als Verkehrsdaten in Bezug auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden, so dürfen diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Der Diensteanbieter muss den Nutzern oder Teilnehmern vor Einholung ihrer Einwilligung mitteilen, welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. ...“

8 In Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) Abs. 1 der Richtlinie 2002/58 heißt es:

„Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie [95/46] für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von

Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 [EUV] niedergelegten Grundsätzen entsprechen.“

Italienisches Recht

Gesetzesvertretendes Dekret Nr. 196/2003

- 9 Art. 132 Abs. 3 des Decreto legislativo n. 196 – Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (gesetzesvertretendes Dekret Nr. 196, Gesetzbuch über den Schutz personenbezogener Daten, mit Bestimmungen zur Anpassung des nationalen Rechts an die Verordnung [EU] 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG) vom 30. Juni 2003 (Supplemento ordinario zu GURI Nr. 174 vom 29. Juli 2003), in seiner auf den Ausgangsrechtsstreit anwendbaren Fassung (im Folgenden: gesetzesvertretendes Dekret Nr. 196/2003) sieht vor:

„Bestehen innerhalb der gesetzlich vorgeschriebenen Aufbewahrungsfrist hinreichende Anhaltspunkte für Straftaten, für die das Gesetz eine lebenslange Freiheitsstrafe oder eine Freiheitsstrafe im Höchstmaß von mindestens drei Jahren vorsieht, die gemäß Art. 4 des [Codice di procedura penale (Strafprozessordnung)] bestimmt wird, oder für Straftaten der Bedrohung, Belästigung oder Störung von Personen per Telefon und handelt es sich um eine ernsthafte Bedrohung, Belästigung oder Störung, so werden die Daten, wenn sie für die Aufklärung des Sachverhalts von Bedeutung sind, auf Antrag der Staatsanwaltschaft oder auf Ersuchen des Verteidigers des Angeklagten, des Beschuldigten, der verletzten Person oder anderer privater Beteiligter erhoben, nachdem der Richter durch mit Gründen versehenen Beschluss die Genehmigung hierzu erteilt hat.“

- 10 Art. 132 Abs. 3-*bis* des gesetzesvertretenden Dekrets Nr. 196/2003 bestimmt:

„Liegen Dringlichkeitsgründe vor und besteht begründeter Verdacht, dass die Ermittlungen durch eine Verzögerung stark beeinträchtigt werden könnten, verfügt die Staatsanwaltschaft die Erhebung der Daten durch mit Gründen versehenen Beschluss, der unverzüglich, jedenfalls aber innerhalb von

48 Stunden, dem zuständigen Richter zur Erteilung der Genehmigung im ordentlichen Verfahren übermittelt wird. Der Richter entscheidet innerhalb der darauffolgenden 48 Stunden durch mit Gründen versehenen Beschluss über die Bestätigung.“

- 11 Ferner dürfen nach Art. 132 Abs. 3-*quater* des gesetzesvertretenden Dekrets Nr. 196/2003 „Daten, die unter Verstoß gegen die Bestimmungen der Abs. 3 und 3-*bis* erhoben wurden, ... nicht verwendet werden“.

Strafgesetzbuch

- 12 Art. 624 („Diebstahl“) des Codice penale (Strafgesetzbuch) bestimmt:

„Wer sich eine fremde bewegliche Sache zueignet, indem er sie dem Gewahrsamsinhaber wegnimmt, um daraus sich oder einem anderen einen Vorteil zu verschaffen, wird mit Freiheitsstrafe von sechs Monaten bis zu drei Jahren sowie mit Geldstrafe in Höhe von 154 bis 516 Euro bestraft.

...

Die Straftat ist auf Antrag des Geschädigten strafbar, es sei denn, eine oder mehrere der in Art. 61 Abs. 7 und Art. 625 genannten Voraussetzungen sind erfüllt.“

- 13 Art. 625 („Erschwerende Umstände“) Abs. 1 des Strafgesetzbuchs sieht vor:

„Die Tat im Sinne von Art. 624 wird mit Freiheitsstrafe von zwei bis sechs Jahren sowie mit Geldstrafe von 927 bis 1 500 Euro bestraft,

...

2. wenn der Täter Gewalt gegen Sachen anwendet oder sich eines betrügerischen Mittels bedient;

3. wenn der Täter Waffen oder Betäubungsmittel bei sich führt, ohne davon Gebrauch zu machen;

4. wenn es sich um einen mit besonderer Geschicklichkeit begangenen Diebstahl handelt;

5. wenn die Tat von drei oder mehr Personen begangen wird oder aber von einer Person, die sich als Amtsträger oder eine mit einem öffentlichen Dienst beauftragte Person verkleidet oder ausgibt;

6. wenn die Tat am Gepäck von Reisenden in Fahrzeugen aller Art, auf Bahnhöfen, Flughäfen oder Bahnsteigen, in Hotels oder in anderen Betrieben, in denen Speisen oder Getränke verkauft werden, begangen wird;

7. wenn die Tat an Sachen in öffentlichen Ämtern oder Anstalten, an beschlagnahmten oder gepfändeten Sachen oder an Sachen begangen wird, die notwendigerweise, gewohnheitsmäßig oder bestimmungsgemäß der Öffentlichkeit zugänglich sind oder für den öffentlichen Dienst, den öffentlichen Gebrauch, die Verteidigung oder die Verehrung bestimmt sind;

7-bis. wenn die Tat an Metallbauteilen oder anderen Werkstoffen begangen wird, die der zur Lieferung von Energie oder zur Erbringung von Verkehrs-, Telekommunikations- oder anderen öffentlichen Dienstleistungen bestimmten und von öffentlichen oder privaten Einrichtungen im Rahmen einer öffentlichen Konzession betriebenen Infrastruktur entzogen werden;

8. wenn die Tat an drei oder mehr zu einer Klein- oder Großviehherde gehörenden Stück Vieh oder an Rindern oder Pferden, auch wenn sie nicht zu einer Herde gehören, begangen wird.

8-bis. wenn die Tat in öffentlichen Verkehrsmitteln begangen wird;

8-ter. wenn die Tat gegenüber einer Person begangen wird, die gerade die Dienste eines Kreditinstituts, einer Postfiliale oder eines Geldautomaten in Anspruch nimmt oder diese Dienste unmittelbar davor in Anspruch genommen hat.“

Strafprozessordnung

- 14 Art. 4 („Vorschriften zur Bestimmung der Zuständigkeit“) Strafprozessordnung lautet:

„Zur Bestimmung der Zuständigkeit ist die gesetzlich für jede vollendete oder versuchte Straftat festgelegte Strafe zu berücksichtigen. Nicht zu berücksichtigen ist, ob es sich um eine fortgesetzte Tat oder einen Wiederholungsfall handelt und unter welchen Umständen die Straftat begangen wird, es sei denn, es handelt sich um erschwerende Umstände, für die das Gesetz eine andere Strafe als die Regelstrafe vorsieht, und Umstände mit besonderen Wirkungen.“

- 15 Art. 269 Abs. 2 der Strafprozessordnung sieht vor:

„... [D]ie Aufzeichnungen [werden] solange aufbewahrt, bis das Urteil rechtskräftig geworden ist. Sofern Unterlagen für das Verfahren nicht benötigt werden, können die Betroffenen jedoch zum Schutz der Privatsphäre bei dem Richter, der das Abhören genehmigt oder bestätigt hat, um Vernichtung von Aufzeichnungen ersuchen.“

Ausgangsrechtsstreit und Vorlagefrage

- 16 Nach der Erstattung zweier Strafanzeigen wegen am 27. Oktober bzw. 20. November 2021 begangener Diebstähle von Mobiltelefonen leitete die Staatsanwaltschaft gemäß den Art. 624 und 625 des Strafgesetzbuchs zwei Strafverfahren gegen Unbekannt wegen schweren Diebstahls ein.
- 17 Zur Ermittlung der Täter dieser Diebstähle beantragte die Staatsanwaltschaft auf der Grundlage von Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 am 7. Dezember bzw. am 30. Dezember 2021 beim vorlegenden Gericht, dem Giudice delle indagini preliminari presso il Tribunale di Bolzano (Ermittlungsrichter beim Landesgericht Bozen), die Genehmigung, bei sämtlichen Telefongesellschaften die Telefonverbindungsdaten der gestohlenen Telefone zu erheben. Die Anträge bezogen sich auf „alle [in Besitz der Telefongesellschaften befindlichen Daten] zwecks Nachverfolgung und Ortung (insbesondere Teilnehmer und eventuell Codes [der internationalen Mobilfunkgeräteerkennung (IMEI) der Anschlüsse], von denen Anrufe ein- und ausgegangen sind, besuchte/aufgerufene Websites, Zeitpunkt und Dauer des Anrufs/der Verbindung sowie Angabe der betroffenen Funkzellen oder Mobilfunkmasten, Teilnehmer und IMEI-Codes [der Anschlüsse], von denen SMS oder MMS gesendet oder empfangen wurden, und, wenn möglich, allgemeine Angaben zu den entsprechenden Anschlussinhabern) der ein- und ausgegangenen Gespräche/Kommunikation per Telefon und hergestellten Verbindungen einschließlich Roaming, auch hinsichtlich nicht in Rechnung gestellter Anrufe (unbeantwortetes Freizeichen), und zwar vom Zeitpunkt des Diebstahls bis zum Zeitpunkt der Antragsstellung“.
- 18 Das vorliegende Gericht hat Zweifel an der Vereinbarkeit von Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 mit Art. 15 Abs. 1 der Richtlinie 2002/58 in seiner Auslegung durch den Gerichtshof im Urteil vom 2. März 2021, Prokuratur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152).
- 19 Es weist darauf hin, dass nach Rn. 45 dieses Urteils nationale Bestimmungen, die den Behörden Zugang zu Telefonverbindungsdaten ermöglichten, die einen Satz von Verkehrs- oder Standortdaten enthielten, aus denen genaue Schlüsse auf das Privatleben des betreffenden Nutzers gezogen werden könnten, in Anbetracht des in Art. 52 Abs. 1 der Charta vorgesehenen Grundsatzes der Verhältnismäßigkeit und der Schwere des Eingriffs in die Grundrechte auf Achtung des Privatlebens, auf den Schutz personenbezogener Daten und auf die Freiheit der Meinungsäußerung und die Informationsfreiheit, wie sie in den Art. 7, 8 und 11 der Charta garantiert seien, nur dann gerechtfertigt werden könnten, wenn sie der Verfolgung schwerer Straftaten, wie etwa ernsthafter Bedrohungen der nationalen Sicherheit, d. h. der Sicherheit des Staates, und anderer schwerer Kriminalität dienten.
- 20 Hierzu habe die Corte suprema di cassazione (Kassationsgerichtshof, Italien) in ihrem Urteil Nr. 33116 vom 7. September 2021 festgestellt, dass diese

Rechtsprechung in Anbetracht des Auslegungsspielraums bei der Entscheidung, welche Straftaten ernsthafte Bedrohungen der nationalen Sicherheit oder andere schwere Kriminalität im Sinne der Rechtsprechung des Gerichtshofs darstellen, nicht die erforderlichen Merkmale aufweise, um von den nationalen Gerichten unmittelbar angewandt zu werden. Infolgedessen habe der italienische Gesetzgeber Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 geändert, indem er Straftaten, die nach dem Gesetz mit einer Freiheitsstrafe im Höchstmaß „von mindestens drei Jahren“ bedroht seien, als schwere Straftaten, zu denen Telefonverbindungsdaten erhoben werden könnten, eingestuft habe.

- 21 Diese Schwelle von drei Jahren Freiheitsstrafe im Höchstmaß zur Ahndung einer Straftat, die rechtfertige, dass es wegen dieser Straftat zu einer Übermittlung der Telefonverbindungsdaten an die Behörden kommen könne, führe dazu, dass diesen diese Verbindungsdaten zur Verfolgung von Straftaten, die nur eine begrenzte sozialschädliche Wirkung entfalten würden und nur auf Antrag einer Privatperson geahndet würden, übermittelt werden könnten, so insbesondere zur Verfolgung von Diebstählen von geringwertigen Sachen wie Diebstählen von Mobiltelefonen oder Fahrrädern.
- 22 Die in Rede stehende nationale Bestimmung verstoße somit gegen den in Art. 52 Abs. 1 der Charta vorgesehenen Grundsatz der Verhältnismäßigkeit, wonach die Schwere der verfolgten Straftat gegen die Grundrechte, in die durch die Verfolgung der Straftat eingegriffen werde, abgewogen werden müsse. Die Rechtfertigung eines Eingriffs in die durch die Art. 7, 8 und 11 der Charta garantierten Grundrechte mit der Verfolgung einer Straftat wie eines Diebstahls stehe nämlich im Widerspruch zu diesem Grundsatz.
- 23 Die italienischen Gerichte verfügten über ein sehr begrenztes Ermessen, die Genehmigung für die Erhebung von Telefonverbindungsdaten zu verweigern, da die Genehmigung nach der in Rede stehenden Bestimmung erteilt werden müsse, wenn „hinreichende Anhaltspunkte für Straftaten“ vorlägen und die angeforderten Daten „für die Aufklärung des Sachverhalts von Bedeutung“ seien. Ein Bewertungsspielraum in Bezug auf die konkrete Schwere einer Straftat, die Gegenstand der Ermittlungen sei, werde den italienischen Gerichten somit nicht eingeräumt. Mit der Regelung, dass die Genehmigung zur Erhebung der Daten namentlich für alle Straftaten zu erteilen sei, die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht seien, sei vom italienischen Gesetzgeber eine abschließende Bewertung vorgenommen worden.
- 24 Unter diesen Umständen hat der Giudice delle indagini preliminari presso il Tribunale di Bolzano (Ermittlungsrichter beim Landesgericht Bozen) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Frage zur Vorabentscheidung vorzulegen:

Steht Art. 15 Abs. 1 der Richtlinie 2002/58 einer nationalen Regelung entgegen, die wie Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 Folgendes vorsieht:

„Bestehen innerhalb der gesetzlich vorgeschriebenen Aufbewahrungsfrist hinreichende Anhaltspunkte für Straftaten, für die das Gesetz eine lebenslange Freiheitsstrafe oder eine Freiheitsstrafe im Höchstmaß von mindestens drei Jahren vorsieht, die gemäß Art. 4 der Strafprozessordnung bestimmt wird, oder für Straftaten der Bedrohung, Belästigung oder Störung von Personen per Telefon und handelt es sich um eine ernsthafte Bedrohung, Belästigung oder Störung, so werden die Daten, falls sie für die Aufklärung des Sachverhalts von Bedeutung sind, auf Antrag der Staatsanwaltschaft oder auf Ersuchen des Verteidigers des Angeklagten, des Beschuldigten, der verletzten Person oder anderer privater Beteiligter erhoben, nachdem der Richter durch mit Gründen versehenen Beschluss die Genehmigung hierzu erteilt hat?“

Zur Zulässigkeit des Vorabentscheidungsersuchens

- 25 Die italienische Regierung und Irland halten das Vorabentscheidungsersuchen für teilweise unzulässig. Die Anträge auf Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten seien von der Staatsanwaltschaft auf der Grundlage von Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 zur Verfolgung schwerer Diebstähle von Mobiltelefonen gestellt worden. Das vorliegende Gericht ersuche den Gerichtshof mit seiner Vorlagefrage jedoch auch um Klärung, ob Art. 15 Abs. 1 der Richtlinie 2002/58 einer nationalen Bestimmung entgegenstehe, die es ermögliche, Zugang zu Daten zu erhalten, die von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert worden seien, um andere unter Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 fallende Straftaten als die im Ausgangsverfahren in Rede stehenden zu verfolgen, wie etwa einen einfachen Diebstahl oder eine ernsthafte Belästigung per Telefon. Soweit sich das Vorabentscheidungsersuchen auf diese anderen Straftaten beziehe, sei es deshalb hypothetisch.
- 26 Insoweit ist es nach ständiger Rechtsprechung im Rahmen der durch Art. 267 AEUV geschaffenen Zusammenarbeit zwischen dem Gerichtshof und den nationalen Gerichten allein Sache des nationalen Gerichts, das mit dem Rechtsstreit befasst ist und in dessen Verantwortungsbereich die zu erlassende Entscheidung fällt, anhand der Besonderheiten der Rechtssache sowohl die Erforderlichkeit einer Vorabentscheidung für den Erlass seines Urteils als auch die Erheblichkeit der dem Gerichtshof vorzulegenden Fragen zu beurteilen. Daher ist der Gerichtshof grundsätzlich gehalten, über ihm vorgelegte Fragen zu befinden, wenn diese die Auslegung des Unionsrechts betreffen (Urteil vom 21. März 2023, Mercedes-Benz Group [Haftung der Hersteller von mit

Abschalteinrichtungen versehenen Fahrzeugen], C-100/21, EU:C:2023:229, Rn. 52 und die dort angeführte Rechtsprechung).

- 27 Infolgedessen spricht eine Vermutung für die Entscheidungserheblichkeit der Fragen zum Unionsrecht. Der Gerichtshof kann die Beantwortung einer Vorlagefrage eines nationalen Gerichts nur ablehnen, wenn die erbetene Auslegung des Unionsrechts offensichtlich in keinem Zusammenhang mit den Gegebenheiten oder dem Gegenstand des Ausgangsrechtsstreits steht, wenn das Problem hypothetischer Natur ist oder wenn der Gerichtshof nicht über die tatsächlichen und rechtlichen Angaben verfügt, die für eine zweckdienliche Beantwortung der ihm vorgelegten Fragen erforderlich sind (Urteil vom 21. März 2023, Mercedes-Benz Group [Haftung der Hersteller von mit Abschalteinrichtungen versehenen Fahrzeugen], C-100/21, EU:C:2023:229, Rn. 53 und die dort angeführte Rechtsprechung).
- 28 Durch die vollständige Wiedergabe von Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 erfasst die Vorlagefrage, auch wenn sie zwischen den Arten von Straftaten, auf die diese Bestimmung anwendbar ist, keine Unterscheidung trifft, zwangsläufig die schweren Diebstähle, für die im Ausgangsverfahren Anträge auf Genehmigung des Zugangs zu personenbezogenen Daten gestellt wurden.
- 29 Die Frage hat folglich keinen hypothetischen Charakter und ist daher zulässig.

Zur Vorlagefrage

- 30 Wie die französische Regierung in ihren schriftlichen Erklärungen ausgeführt hat, wird der Gerichtshof mit der Frage des vorlegenden Gerichts, so wie sie formuliert ist, ersucht, sich zur Vereinbarkeit von Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 mit Art. 15 Abs. 1 der Richtlinie 2002/58 zu äußern.
- 31 Hierzu ist darauf hinzuweisen, dass der Gerichtshof im Rahmen des durch Art. 267 AEUV geschaffenen Verfahrens weder zur Auslegung innerstaatlicher Rechts- oder Verwaltungsvorschriften noch zu Äußerungen über deren Vereinbarkeit mit dem Unionsrecht befugt ist. Nach ständiger Rechtsprechung kann der Gerichtshof nämlich im Rahmen eines Vorabentscheidungsersuchens nach Art. 267 AEUV nur das Unionsrecht in den Grenzen der der Union übertragenen Zuständigkeiten auslegen (Urteil vom 14. Dezember 2023, Getin Noble Bank [Verjährungsfrist für Rückgewähransprüche], C-28/22, EU:C:2023:992, Rn. 53 und die dort angeführte Rechtsprechung).
- 32 Andererseits obliegt es nach ständiger Rechtsprechung dem Gerichtshof, im Fall ungenau formulierter oder den Rahmen seiner Befugnisse nach Art. 267 AEUV überschreitender Fragen aus dem gesamten vom nationalen Gericht vorgelegten Material, insbesondere der Begründung der Vorlageentscheidung,

diejenigen Elemente des Unionsrechts herauszuarbeiten, die angesichts des Gegenstands des Rechtsstreits einer Auslegung bedürfen. Hierzu hat der Gerichtshof die ihm vorgelegten Fragen gegebenenfalls umzuformulieren (Urteil vom 14. Dezember 2023, Sparkasse Südpfalz, C-206/22, EU:C:2023:984, Rn. 20 und die dort angeführte Rechtsprechung).

- 33 Außerdem kann der Gerichtshof veranlasst sein, unionsrechtliche Vorschriften zu berücksichtigen, die das nationale Gericht in seiner Frage nicht angeführt hat (Urteil vom 17. November 2022, Harman International Industries, C-175/21, EU:C:2022:895, Rn. 31 und die dort angeführte Rechtsprechung).
- 34 Nach alledem ist davon auszugehen, dass das vorlegende Gericht mit seiner Frage im Wesentlichen wissen möchte, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Bestimmung entgegensteht, die ein nationales Gericht, das im Rahmen einer vorherigen Kontrolle tätig wird, die aufgrund eines im Rahmen strafrechtlicher Ermittlungen gestellten und mit Gründen versehenen Antrags einer zuständigen nationalen Behörde auf Zugang zu einem Satz von Verkehrs- oder Standortdaten erfolgt, die von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert wurden und aus denen genaue Schlüsse auf das Privatleben des betreffenden Nutzers eines elektronischen Kommunikationsmittels gezogen werden können, verpflichtet, diesen Zugang zu genehmigen, wenn der Zugang zum Zweck der Ermittlung von Straftaten beantragt wird, die im nationalen Recht mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht sind, sofern hinreichende Anhaltspunkte für solche Straftaten bestehen und diese Daten für die Aufklärung des Sachverhalts von Bedeutung sind.
- 35 Zu den Voraussetzungen, unter denen Behörden in Anwendung einer gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassenen Rechtsvorschrift zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Verkehrs- und Standortdaten eingeräumt werden darf, hat der Gerichtshof entschieden, dass ein solcher Zugang nur gewährt werden darf, wenn diese Daten von den Betreibern in einer mit Art. 15 Abs. 1 im Einklang stehenden Weise gespeichert wurden (vgl. in diesem Sinne Urteil vom heutigen Tag, La Quadrature du Net u. a. [Personenbezogene Daten und Bekämpfung von Verletzungen der Rechte des geistigen Eigentums], C-470/21, Rn. 65 sowie die dort angeführte Rechtsprechung). Er hat ferner entschieden, dass der genannte Art. 15 Abs. 1 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta Rechtsvorschriften entgegensteht, die zu solchen Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen (Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu elektronischen Kommunikationsdaten], C-746/18, EU:C:2021:152, Rn. 30 und die dort angeführte Rechtsprechung).

- 36 Ferner ist auf die Rechtsprechung des Gerichtshofs hinzuweisen, wonach nur die Ziele der Bekämpfung schwerer Kriminalität oder der Verhütung ernsthafter Bedrohungen der öffentlichen Sicherheit einen schweren Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte rechtfertigen, der sich aus dem Zugang der Behörden zu einem Satz von Verkehrs- oder Standortdaten ergibt, die geeignet sind, Informationen über die Kommunikation eines Nutzers eines elektronischen Kommunikationsmittels oder über den Standort der von ihm verwendeten Endgeräte zu liefern, aus denen genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden können, ohne dass andere die Verhältnismäßigkeit eines Zugangsanspruchs betreffende Faktoren wie die Länge des Zeitraums, für den der Zugang zu solchen Daten begehrt wird, dazu führen können, dass das Ziel, Straftaten allgemein zu verhüten, zu ermitteln, festzustellen und zu verfolgen, einen solchen Zugang zu rechtfertigen vermag (vgl. in diesem Sinne Urteil vom 2. März 2021, Prokuratur [Voraussetzungen für den Zugang zu elektronischen Kommunikationsdaten], C-746/18, EU:C:2021:152, Rn. 35 und die dort angeführte Rechtsprechung).
- 37 Mit seiner Vorlagefrage möchte das vorlegende Gericht im Wesentlichen wissen, ob ein solcher schwerer Eingriff bei Straftaten wie denjenigen, auf die sich die im Ausgangsverfahren in Rede stehende nationale Regelung bezieht, genehmigt werden kann.
- 38 Zur Einstufung eines Zugangs wie des im Ausgangsrechtsstreit in Rede stehenden als schwerer Eingriff in die in den Art. 7 und 8 der Charta garantierten Grundrechte, ist zunächst festzustellen, dass die Staatsanwaltschaft zur Ermittlung der Täter der mutmaßlichen Diebstähle, die diesem Rechtsstreit zugrunde liegen, für jedes der betroffenen Mobiltelefone beim vorlegenden Gericht auf der Grundlage von Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 die Genehmigung beantragt hat, alle im Besitz der Telefongesellschaften befindlichen Daten zu erheben, die mittels einer Methode zur Nachverfolgung und Ortung der Gespräche und Telefonverbindungen sowie der mit diesen Telefonanschlüssen hergestellten Verbindungen gewonnen wurden. Die Anträge betrafen insbesondere die Teilnehmer und IMEI-Codes der Anschlüsse, von denen Anrufe ein- und ausgegangen sind, die besuchten/aufgerufenen Websites, den Zeitpunkt und die Dauer des Anrufs/der Verbindung, die Angabe der betroffenen Funkzellen oder Mobilfunkmasten sowie der Teilnehmer und IMEI-Codes der Anschlüsse, von denen SMS oder MMS gesendet oder empfangen wurden.
- 39 Der Zugang zu einem solchen Satz von Verkehrs- oder Standortdaten kann es ermöglichen, genaue Schlüsse auf das Privatleben der Personen zu ziehen, deren Daten gespeichert wurden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren

(vgl. in diesem Sinne Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu elektronischen Kommunikationsdaten], C-746/18, EU:C:2021:152, Rn. 36 und die dort angeführte Rechtsprechung). Der durch den Zugang zu solchen Daten verursachte Eingriff in die in den Art. 7 und 8 der Charta garantierten Grundrechte kann daher als schwerer Eingriff eingestuft werden.

- 40 Wie sich aus Rn. 39 des Urteils vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152), ergibt, kann diese Bewertung nicht allein deshalb verworfen werden, weil die beiden in Rede stehenden Anträge auf Zugang zu Verkehrs- oder Standortdaten nur kurze Zeiträume von weniger als zwei Monaten betrafen, die von den Zeitpunkten der mutmaßlichen Diebstähle der Mobiltelefone bis zu den Zeitpunkten reichen, zu denen diese Anträge gestellt wurden, da die Anträge einen Satz dieser Daten betrafen, die genaue Informationen über das Privatleben der Personen liefern können, die die betreffenden Mobiltelefone nutzen.
- 41 Zudem ist für die Bewertung, ob ein schwerer Eingriff in die durch die Art. 7 und 8 der Charta garantierten Rechte vorliegt, der Umstand unerheblich, dass es sich bei den Daten, zu denen die Staatsanwaltschaft den Zugang beantragt hat, nicht um die Daten der Eigentümer der in Rede stehenden Mobiltelefone handelt, sondern um die Daten der Personen, die miteinander kommuniziert haben, indem sie diese Telefone nach deren mutmaßlichen Diebstählen benutzt haben. Aus Art. 5 Abs. 1 der Richtlinie 2002/58 geht nämlich hervor, dass sich die grundsätzliche Verpflichtung, die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten sowie die Vertraulichkeit der damit verbundenen Verkehrsdaten sicherzustellen, auf die Kommunikation der Nutzer dieses Netzes bezieht. Der Ausdruck „Nutzer“ bezeichnet nach Art. 2 Buchst. a dieser Richtlinie eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben.
- 42 In Anbetracht der in Rn. 36 des vorliegenden Urteils angeführten Rechtsprechung, wonach Eingriffe in Grundrechte, die durch den Zugang zu Daten, wie sie im Ausgangsverfahren in Rede stehen, verursacht werden, als schwer angesehen werden können, lassen sich diese Eingriffe daher nur durch die Ziele der Bekämpfung schwerer Kriminalität oder der Verhütung ernsthafter Bedrohungen der öffentlichen Sicherheit rechtfertigen.
- 43 Sodann sind zwar die Voraussetzungen, unter denen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den ihnen zur Verfügung stehenden Daten gewähren müssen, im nationalen Recht festzulegen, jedoch muss eine solche Regelung klare und präzise Regeln für den Umfang und die Voraussetzungen für einen solchen

Zugang enthalten. Dieser Zugang kann im Zusammenhang mit dem Ziel der Bekämpfung von Kriminalität grundsätzlich nur zu Daten von Personen gewährt werden, die im Verdacht stehen, in eine schwere Straftat verwickelt zu sein. Um in der Praxis die vollständige Einhaltung dieser Voraussetzungen, die sicherstellen, dass der Eingriff auf das absolut Notwendige beschränkt bleibt, zu gewährleisten, ist es unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird (vgl. in diesem Sinne Urteil vom 2. März 2021, Prokuratour [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 48 bis 51).

- 44 Was schließlich die Definition des Begriffs „schwere Straftat“ betrifft, ergibt sich aus der Rechtsprechung, dass das Strafrecht und die Regeln des Strafverfahrens, soweit die Union in diesem Bereich keine Rechtsvorschriften erlassen hat, in die Zuständigkeit der Mitgliedstaaten fallen. Diese müssen von dieser Zuständigkeit jedoch unter Wahrung des Unionsrechts Gebrauch machen (vgl. in diesem Sinne Urteil vom 26. Februar 2019, Rimšēvičs und EZB/Lettland, C-202/18 und C-238/18, EU:C:2019:139, Rn. 57 sowie die dort angeführte Rechtsprechung).
- 45 Insofern ist darauf hinzuweisen, dass die Definition der Straftaten, der strafmildernden und -erschwerenden Umstände und der Strafen sowohl die sozialen Gegebenheiten als auch die Rechtstraditionen widerspiegelt, die nicht nur von Mitgliedstaat zu Mitgliedstaat, sondern auch im Lauf der Zeit variieren. Diesen Gegebenheiten und Traditionen kommt somit eine gewisse Bedeutung für die Entscheidung zu, welche Straftaten als schwere Straftaten angesehen werden.
- 46 Angesichts der Verteilung der Zuständigkeiten zwischen der Union und den Mitgliedstaaten nach dem AEU-Vertrag und der erheblichen Unterschiede zwischen den Rechtssystemen der Mitgliedstaaten im Bereich des Strafrechts ist deshalb davon auszugehen, dass die Definition „schwerer Straftaten“ für die Anwendung von Art. 15 Abs. 1 der Richtlinie 2002/58 Sache der Mitgliedstaaten ist.
- 47 Die von den Mitgliedstaaten vorgenommene Definition der „schweren Straftaten“ muss allerdings den Anforderungen entsprechen, die sich aus Art. 15 Abs. 1 der Richtlinie 2002/58 in Verbindung mit den Art. 7, 8 und 11 sowie aus Art. 52 Abs. 1 der Charta ergeben.
- 48 Indem Art. 15 Abs. 1 der Richtlinie 2002/58 den Mitgliedstaaten gestattet, Rechtsvorschriften zu erlassen, die die Rechte und Pflichten gemäß u. a. den Art. 5, 6 und 9 dieser Richtlinie – wie sie sich aus den Grundsätzen der Vertraulichkeit der Kommunikation und dem Verbot der Speicherung der damit

verbundenen Daten ergeben – „beschränken“, sieht diese Bestimmung eine Ausnahme von der allgemeinen Regel vor, die u. a. in den Art. 5, 6 und 9 der Richtlinie vorgesehen ist, und ist daher nach ständiger Rechtsprechung eng auszulegen. Eine solche Bestimmung vermag es daher nicht zu rechtfertigen, dass die Ausnahme von der grundsätzlichen Verpflichtung, die Vertraulichkeit der elektronischen Kommunikation und der damit verbundenen Daten sicherzustellen, zur Regel wird, soll Art. 5 der Richtlinie nicht weitgehend ausgehöhlt werden (vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 40).

- 49 Außerdem geht aus Art. 15 Abs. 1 Satz 3 der Richtlinie 2002/58 hervor, dass die nach dieser Vorschrift von den Mitgliedstaaten erlassenen Vorschriften die allgemeinen Grundsätze der Union beachten müssen, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und die Achtung der durch die Art. 7, 8 und 11 der Charta garantierten Grundrechte gewährleisten müssen (vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 42).
- 50 Demnach dürfen die Mitgliedstaaten den Begriff „schwere Straftat“ und im weiteren Sinne den Begriff „schwere Kriminalität“ nicht dadurch verfälschen, dass sie für die Anwendung von Art. 15 Abs. 1 der Richtlinie 2002/58 Straftaten einbeziehen, bei denen es sich angesichts der vorherrschenden gesellschaftlichen Bedingungen in dem betreffenden Mitgliedstaat offensichtlich nicht um schwere Straftaten handelt, auch wenn der Gesetzgeber dieses Mitgliedstaats vorgesehen hat, sie mit einer Freiheitsstrafe im Höchstmaß von drei Jahren zu bedrohen.
- 51 Vor allem im Hinblick auf eine Prüfung, dass keine solche Verfälschung vorliegt, ist es von wesentlicher Bedeutung, dass der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten, wenn er die Gefahr eines schweren Eingriffs in die Grundrechte der betroffenen Person birgt, einer vorherigen Kontrolle durch ein Gericht oder durch eine unabhängige Verwaltungsstelle unterworfen wird (vgl. in diesem Sinne Urteil vom heutigen Tag, La Quadrature du Net u. a. [Personenbezogene Daten und Bekämpfung von Verletzungen der Rechte des geistigen Eigentums], C-470/21, Rn. 124 bis 131).
- 52 Im vorliegenden Fall geht aus der Vorlageentscheidung hervor, dass Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 die Voraussetzungen festlegt, unter denen ein Gericht, das mit einem mit Gründen versehenen Antrag einer Behörde befasst ist, Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten gewähren kann. Diese Bestimmung definiert unter Bezugnahme auf eine Freiheitsstrafe im Höchstmaß von mindestens drei Jahren die Straftaten, für die der Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten gewährt werden kann. Sie macht diesen Zugang von der

doppelten Voraussetzung abhängig, dass „hinreichende Anhaltspunkte für eine Straftat“ vorliegen und dass diese Daten „für die Aufklärung des Sachverhalts von Bedeutung“ sind.

- 53 Das vorliegende Gericht fragt sich jedoch, ob die sich aus dieser Bestimmung ergebende Definition der „schweren Straftaten“, für deren Verfolgung Zugang zu den Daten gewährt werden kann, nicht zu weit geht, da sie Straftaten erfasst, die nur eine begrenzte sozialschädliche Wirkung entfalten.
- 54 Hierzu ist erstens festzustellen, dass sich eine Definition, wonach „schwere Straftaten“, für deren Verfolgung der Zugang gewährt werden kann, solche sind, für die die Freiheitsstrafe im Höchstmaß mindestens eine gesetzlich bestimmte Dauer beträgt, auf ein objektives Kriterium stützt. Dies steht im Einklang mit dem Erfordernis, dass sich die betreffenden nationalen Rechtsvorschriften bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugang zu den fraglichen Daten zu gewähren ist, auf objektive Kriterien stützen müssen (Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 105 sowie die dort angeführte Rechtsprechung).
- 55 Zweitens ergibt sich aus der in Rn. 48 des vorliegenden Urteils angeführten Rechtsprechung, dass eine im nationalen Recht vorgenommene Definition „schwerer Straftaten“, die einen Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten, aus denen genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden können, ermöglichen können, nicht so weit sein darf, dass der Zugang zu diesen Daten eher zur Regel als zur Ausnahme wird. Sie kann daher nicht den Großteil der Straftaten erfassen, was der Fall wäre, wenn die Schwelle, bei deren Überschreitung die Freiheitsstrafe im Höchstmaß, mit der eine Straftat bedroht ist, es rechtfertigt, diese als schwere Straftat einzustufen, übermäßig niedrig angesetzt wäre.
- 56 Eine Schwelle, die unter Bezugnahme auf eine Freiheitsstrafe im Höchstmaß von drei Jahren festgelegt wird, ist insoweit jedoch nicht als übermäßig niedrig anzusehen (vgl. in diesem Sinne Urteil vom 21. Juni 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, Rn. 150).
- 57 Da die Definition „schwerer Straftaten“, für die der Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten verlangt werden kann, nicht unter Bezugnahme auf eine anwendbare Mindeststrafe, sondern auf eine anwendbare Höchststrafe festgelegt wird, ist es zwar nicht ausgeschlossen, dass ein Zugang zu Daten, der einen schweren Eingriff in die Grundrechte darstellt, für die Verfolgung von Straftaten, die in Wirklichkeit nicht zur schweren Kriminalität gehören, beantragt werden kann (vgl. entsprechend Urteil vom 21. Juni 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, Rn. 151).

- 58 Die Festlegung einer Schwelle, ab der die für die Ahndung einer Straftat vorgesehene Freiheitsstrafe im Höchstmaß es rechtfertigt, diese Straftat als schwere Straftat einzustufen, verstößt jedoch nicht zwangsläufig gegen den Grundsatz der Verhältnismäßigkeit.
- 59 Dies gilt zum einen für eine Bestimmung wie die im Ausgangsverfahren in Rede stehende, da sie, wie aus der Vorlageentscheidung hervorgeht, allgemein den Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten betrifft, ohne die Art dieser Daten näher zu bestimmen. Offenbar erfasst diese Bestimmung somit u. a. Fälle, in denen der Zugang nicht als schwerer Eingriff eingestuft werden kann, da er sich nicht auf einen Satz von Daten bezieht, aus denen genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden können.
- 60 Zum anderen müssen Gerichte bzw. unabhängige Verwaltungsstellen, die im Rahmen einer vorherigen Kontrolle aufgrund eines mit Gründen versehenen Antrags tätig werden, befugt sein, diesen Zugang zu verweigern oder einzuschränken, wenn sie feststellen, dass ein solcher Zugang einen schweren Eingriff in die Grundrechte darstellen würde, und demgegenüber offensichtlich ist, dass die betreffende Straftat tatsächlich nicht zur schweren Kriminalität gehört (vgl. entsprechend Urteil vom 21. Juni 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, Rn. 152).
- 61 Die mit der Kontrolle betrauten Gerichte oder Stellen müssen nämlich in der Lage sein, für einen gerechten Ausgleich zwischen den berechtigten Interessen, die sich aus den Erfordernissen von Ermittlungen im Rahmen der Kriminalitätsbekämpfung ergeben, und den Grundrechten auf Achtung des Privatlebens und auf Schutz personenbezogener Daten der Personen, auf deren Daten zugegriffen wird, zu sorgen (Urteil vom heutigen Tag, La Quadrature du Net u. a. [Persönliche Daten und Bekämpfung von Verletzungen der Rechte des geistigen Eigentums], C-470/21, Rn. 125 und die dort angeführte Rechtsprechung).
- 62 Insbesondere müssen diese Gerichte oder Stellen im Rahmen ihrer Prüfung der Verhältnismäßigkeit des Eingriffs in die Grundrechte der vom Antrag auf Zugang betroffenen Person in der Lage sein, einen solchen Zugang auszuschließen, wenn er im Rahmen der Verfolgung einer Straftat begehrt wird, bei der es sich offensichtlich nicht um eine schwere Straftat im Sinne von Rn. 50 des vorliegenden Urteils handelt.
- 63 Nach alledem ist auf die Vorlagefrage zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Bestimmung nicht entgegensteht, die ein nationales Gericht, das im Rahmen einer vorherigen Kontrolle tätig wird, die aufgrund eines im Rahmen strafrechtlicher Ermittlungen gestellten und mit Gründen versehenen Antrags einer zuständigen

nationalen Behörde auf Zugang zu einem Satz von Verkehrs- oder Standortdaten erfolgt, die von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert wurden und aus denen genaue Schlüsse auf das Privatleben des betreffenden Nutzers eines elektronischen Kommunikationsmittels gezogen werden können, verpflichtet, diesen Zugang zu genehmigen, wenn der Zugang zum Zweck der Ermittlung von Straftaten beantragt wird, die im nationalen Recht mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht sind, sofern hinreichende Anhaltspunkte für solche Straftaten bestehen und diese Daten für die Aufklärung des Sachverhalts von Bedeutung sind, vorausgesetzt allerdings, dass das Gericht befugt ist, den Zugang zu verweigern, wenn er im Rahmen von Ermittlungen zu einer Straftat begehrt wird, bei der es sich angesichts der im betreffenden Mitgliedstaat vorherrschenden gesellschaftlichen Bedingungen offensichtlich nicht um eine schwere Straftat handelt.

Kosten

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

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

Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union

dahin auszulegen, dass

er einer nationalen Bestimmung nicht entgegensteht, die ein nationales Gericht, das im Rahmen einer vorherigen Kontrolle tätig wird, die aufgrund eines im Rahmen strafrechtlicher Ermittlungen gestellten und mit Gründen versehenen Antrags einer zuständigen nationalen Behörde auf Zugang zu einem Satz von Verkehrs- oder Standortdaten erfolgt, die von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert wurden und aus denen genaue Schlüsse auf das Privatleben des betreffenden Nutzers eines elektronischen Kommunikationsmittels gezogen werden können, verpflichtet, diesen Zugang zu genehmigen, wenn der Zugang zum Zweck der Ermittlung von Straftaten beantragt wird, die

im nationalen Recht mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht sind, sofern hinreichende Anhaltspunkte für solche Straftaten bestehen und diese Daten für die Aufklärung des Sachverhalts von Bedeutung sind, vorausgesetzt allerdings, dass das Gericht befugt ist, den Zugang zu verweigern, wenn er im Rahmen von Ermittlungen zu einer Straftat begehrt wird, bei der es sich angesichts der im betreffenden Mitgliedstaat vorherrschenden gesellschaftlichen Bedingungen offensichtlich nicht um eine schwere Straftat handelt.