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

URTEIL DES GERICHTSHOFS (Erste Kammer)

7. September 2023(*)

„Vorlage zur Vorabentscheidung – Telekommunikation – Verarbeitung personenbezogener Daten in der elektronischen Kommunikation – Richtlinie 2002/58/EG – Geltungsbereich – Art. 15 Abs. 1 – Von Betreibern elektronischer Kommunikationsdienste gespeicherte und mit Strafverfahren befassten Behörden zur Verfügung gestellte Daten – Spätere Nutzung der Daten bei Ermittlungen wegen eines Dienstvergehens“

In der Rechtssache C-162/22

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Lietuvos vyriausiasis administracinis teismas (Oberstes Verwaltungsgericht, Litauen) mit Entscheidung vom 24. Februar 2022, beim Gerichtshof eingegangen am 3. März 2022, in dem Verfahren

A. G.,

Beteiligte:

Lietuvos Respublikos generalinė prokuratūra,

erlässt

DER GERICHTSHOF (Erste Kammer)

unter Mitwirkung des Kammerpräsidenten A. Arabadjiev, der Richter P. G. Xuereb (Berichterstatter), T. von Danwitz und A. Kumin sowie der Richterin I. Ziemele,

Generalanwalt: M. Campos Sánchez-Bordona,

Kanzler: A. Lamote, Verwaltungsrätin,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 2. Februar 2023,

unter Berücksichtigung der Erklärungen

– von A. G., vertreten durch G. Danėlius, Advokatas,

– der litauischen Regierung, vertreten durch S. Grigonis, V. Kazlauskaitė-Švenčionienė und V. Vasiliauskienė als Bevollmächtigte,

– der tschechischen Regierung, vertreten durch O. Serdula, M. Smolek und J. Vláčil als Bevollmächtigte,

– der estnischen Regierung, vertreten durch M. Kriisa als Bevollmächtigte,

– Irlands, vertreten durch M. Browne, A. Joyce und M. Tierney als Bevollmächtigte im Beistand von D. Fennelly, BL,

– der französischen Regierung, vertreten durch R. Bénard als Bevollmächtigten,

– der italienischen Regierung, vertreten durch G. Palmieri als Bevollmächtigte im Beistand von A. Grumetto, Avvocato dello Stato,

– der ungarischen Regierung, vertreten durch Zs. Biró-Tóth und M. Z. Fehér als Bevollmächtigte,

– der Europäischen Kommission, vertreten durch S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal und F. Wilman als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 30. März 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).

2 Es ergeht im Rahmen eines von A. G. angestrengten Verfahrens wegen der Rechtmäßigkeit von Entscheidungen der Lietuvos Respublikos generalinė prokuratūra (Generalstaatsanwaltschaft der Republik Litauen, im Folgenden: Generalstaatsanwaltschaft), mit denen A. G. seines Amtes als Staatsanwalt enthoben wurde.

Rechtlicher Rahmen

Unionsrecht

3 In Art. 1 („Geltungsbereich und Zielsetzung“) der Richtlinie 2002/58 heißt es:

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

…

(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.“

4 Art. 5 („Vertraulichkeit der Kommunikation“) der Richtlinie sieht in Abs. 1 vor:

„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.“

5 Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG“) der Richtlinie bestimmt in Abs. 1:

„Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/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)] 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."

Litauisches Recht

Gesetz über die elektronische Kommunikation

6 Nach Art. 65 Abs. 2 des Lietuvos Respublikos elektroninių ryšių įstatymas (Gesetz der Republik Litauen über die elektronische Kommunikation) vom 15. April 2004 (Žin., 2004, Nr. 69-2382) in seiner auf den Sachverhalt des Ausgangsverfahrens anwendbaren Fassung (im Folgenden: Gesetz über die elektronische Kommunikation) sind die Betreiber elektronischer Kommunikationsdienste verpflichtet, die in Anhang 1 des Gesetzes aufgeführten Daten auf Vorrat zu speichern und sie gegebenenfalls den zuständigen Behörden zur Verfügung zu stellen, damit diese sie zur Bekämpfung schwerer Kriminalität nutzen können.

7 Nach Anhang 1 des Gesetzes über die elektronische Kommunikation sind folgende Kategorien von Daten zu speichern:

„1. zur Rückverfolgung und Identifizierung der Quelle einer Kommunikation benötigte Daten: … 2. zur Identifizierung des Adressaten einer Kommunikation benötigte Daten: … 3. zur Bestimmung von Datum, Uhrzeit und Dauer einer Kommunikation benötigte Daten: … 4. zur Bestimmung der Art einer Kommunikation benötigte Daten: … 5. zur Bestimmung der Endeinrichtung oder der möglichen Endeinrichtung der Benutzer benötigte Daten: … 6. zur Bestimmung des Standorts mobiler Geräte benötigte Daten: …"

8 Nach Art. 77 Abs. 4 des Gesetzes müssen die Betreiber elektronischer Kommunikationsdienste, wenn eine mit Gründen versehene gerichtliche Entscheidung oder eine andere Rechtsgrundlage sie dazu ermächtigt, insbesondere den mit strafrechtlichen Ermittlungen und Untersuchungen betrauten Behörden gemäß den Vorschriften des Lietuvos Respublikos baudžiamojo proceso kodeksas (Strafprozessordnung der Republik Litauen, im Folgenden: Strafprozessordnung) die Kontrolle des Inhalts der durch elektronische Kommunikationsnetze übermittelten Informationen ermöglichen.

Gesetz über die kriminalpolizeiliche Erkenntnisgewinnung

9 Nach Art. 6 Abs. 3 Nr. 1 des Lietuvos Respublikos kriminalinės žvalgybos įstatymas (Gesetz der Republik Litauen über die kriminalpolizeiliche Erkenntnisgewinnung) vom 2. Oktober 2012 (Žin., 2012, Nr. 122-6093) in seiner auf den Sachverhalt des Ausgangsverfahrens anwendbaren Fassung (im Folgenden: Gesetz über die kriminalpolizeiliche Erkenntnisgewinnung) sind, wenn die in diesem Gesetz vorgesehenen Voraussetzungen für eine kriminalpolizeiliche Erkenntnisgewinnung vorliegen und eine staatsanwaltliche oder gerichtliche Genehmigung eingeholt wurde, neben den in den Abs. 1 und 2 dieses Artikels genannten Behörden die mit strafrechtlichen Ermittlungen betrauten Behörden befugt, bei den Betreibern elektronischer Kommunikationsdienste Informationen einzuholen.

10 Art. 8 Abs. 1 dieses Gesetzes sieht vor, dass die mit strafrechtlichen Ermittlungen betrauten Behörden u. a. tätig werden, sobald ihnen Informationen über die Vorbereitung oder Begehung einer besonders schweren, schweren oder minder schweren Straftat oder über Personen vorliegen, die eine solche Straftat vorbereiten, begehen oder begangen haben. Nach Art. 8 Abs. 3 werden, wenn die Untersuchung Anhaltspunkte für das Vorliegen einer Straftat ergibt, unverzüglich strafrechtliche Ermittlungen eingeleitet.

11 Nach Art. 19 Abs. 1 Nr. 5 des Gesetzes über die kriminalpolizeiliche Erkenntnisgewinnung dürfen die bei strafrechtlichen Ermittlungen gewonnenen Informationen in den Fällen genutzt werden, die in Art. 19 Abs. 3 und 4 aufgeführt oder in anderen Rechtsvorschriften vorgesehen sind. Nach Art. 19 Abs. 3 können Informationen über einen Sachverhalt, der die Merkmale einer mit Korruption im Zusammenhang stehenden Straftat aufweist, mit Einverständnis der Staatsanwaltschaft offengelegt und im Rahmen von Ermittlungen wegen Disziplinar- oder Dienstvergehen genutzt werden.

Strafprozessordnung

12 Art. 154 der Strafprozessordnung sieht vor, dass eine Ermittlungsbehörde auf der Grundlage eines auf Antrag der Staatsanwaltschaft erlassenen gerichtlichen Beschlusses über elektronische Kommunikationsmedien übermittelte Gespräche abhören und registrieren lassen sowie andere über diese Netze übermittelte Informationen kontrollieren, aufzeichnen und speichern kann, wenn Gründe für die Annahme vorliegen, dass dadurch Daten über eine geplante, gegenwärtige oder vollendete besonders schwere oder schwere Straftat oder über eine minder schwere oder leichte Straftat erlangt werden können.

13 Nach Art. 177 Abs. 1 der Strafprozessordnung sind die Daten aus dem Ermittlungsverfahren vertraulich und dürfen bis zur gerichtlichen Prüfung der Strafsache nur mit Genehmigung der Staatsanwaltschaft und nur im gerechtfertigten Umfang offengelegt werden.

14 Die Durchführung von Art. 177 der Strafprozessordnung ist in den Ikiteismino tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteismino tyrimo duomenų apsaugos rekomendacijos (Empfehlungen zur Bereitstellung und Nutzung von Daten aus dem Ermittlungsverfahren für nicht strafrechtliche Zwecke und zum Schutz dieser Daten) geregelt, die durch die Anordnung Nr. I-279 des Generalstaatsanwalts vom 17. August 2017 (TAR, 2017, Nr. 2017-13413), zuletzt geändert durch die Anordnung Nr. I-211 vom 25. Juni 2018, genehmigt wurden.

15 Nach Nr. 23 dieser Empfehlungen entscheidet der Staatsanwalt, wenn er einen Antrag auf Zugang zu Daten aus dem Ermittlungsverfahren erhält, über deren Bereitstellung. Gibt er dem Antrag statt, muss er angeben, auf welche Weise die angeforderten Daten bereitgestellt werden können.

Ausgangsverfahren und Vorlagefrage

16 Die Generalstaatsanwaltschaft leitete gegen den Kläger des Ausgangsverfahrens, der seinerzeit das Amt eines Staatsanwalts bei einer litauischen Staatsanwaltschaft innehatte, eine behördliche Untersuchung ein, weil es Anhaltspunkte dafür gab, dass er im Rahmen von ihm geleiteter Ermittlungen dem Verdächtigen und seinem Anwalt rechtswidrig relevante Informationen zu diesem Verfahren gegeben hatte.

17 In ihrem Bericht über diese Untersuchung kam die Generalstaatsanwaltschaft zu dem Ergebnis, dass dem Kläger des Ausgangsverfahrens ein Dienstvergehen anzulasten sei.

18 Nach den Angaben in diesem Bericht wurde das Dienstvergehen durch die bei der behördlichen Untersuchung ermittelten Tatsachen belegt. Insbesondere hätten die von der Kriminalpolizei gewonnenen Erkenntnisse und die bei zwei strafrechtlichen Ermittlungsverfahren gesammelten Daten bestätigt, dass es Telefonate zwischen dem Kläger des Ausgangsverfahrens und dem Anwalt des Verdächtigen im Rahmen der gegen ihn gerichteten und vom Kläger des Ausgangsverfahrens geleiteten Ermittlungen gegeben habe. In dem Bericht heißt es ferner, dass durch gerichtliche Beschlüsse die Überwachung und Aufzeichnung des Inhalts der über elektronische Kommunikationsnetze übermittelten Informationen bei dem betreffenden Anwalt und beim Kläger des Ausgangsverfahrens genehmigt worden seien.

19 Auf der Grundlage dieses Berichts erließ die Generalstaatsanwaltschaft zwei Anordnungen, mit denen sie gegen den Kläger des Ausgangsverfahrens eine Sanktion in Form der Entlassung aus dem Dienst verhängte und ihn seines Amtes enthob.

20 Der Kläger des Ausgangsverfahrens erhob beim Vilniaus apygardos administracinis teismas (Regionalverwaltungsgericht Vilnius, Litauen) Klage u. a. auf Aufhebung dieser beiden Anordnungen.

21 Mit Urteil vom 16. Juli 2021 wies dieses Gericht seine Klage u. a. mit der Begründung ab, dass die Kriminalpolizei im vorliegenden Fall rechtmäßig vorgegangen sei und dass die im Einklang mit den Bestimmungen des Gesetzes über die kriminalpolizeiliche Erkenntnisgewinnung gesammelten Informationen rechtmäßig genutzt worden seien, um zu beurteilen, ob ihm ein Dienstvergehen anzulasten sei.

22 Der Kläger des Ausgangsverfahrens legte ein Rechtsmittel beim Lietuvos vyriausiasis administracinis teismas (Oberstes Verwaltungsgericht von Litauen), dem vorlegenden Gericht, ein und machte geltend, der Zugang der Ermittlungsbehörden zu Verkehrsdaten und sogar zum Inhalt der elektronischen Kommunikation im Rahmen kriminalpolizeilicher Ermittlungen stelle einen so schwerwiegenden Eingriff in die Grundrechte dar, dass er in Anbetracht der Bestimmungen der Richtlinie 2002/58 und der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) nur zur Bekämpfung schwerer Straftaten gewährt werden dürfe. Art. 19 Abs. 3 des Gesetzes über die kriminalpolizeiliche Erkenntnisgewinnung sehe aber vor, dass solche Daten nicht nur bei Ermittlungen wegen schwerer Straftaten, sondern auch bei Disziplinar- oder Dienstvergehen im Zusammenhang mit Korruption genutzt werden könnten.

23 Nach den Angaben des vorlegenden Gerichts betreffen die vom Kläger des Ausgangsverfahrens aufgeworfenen Fragen zwei Gesichtspunkte, und zwar zum einen den Zugang zu Daten, die von Betreibern elektronischer Kommunikationsdienste zu anderen Zwecken als der Bekämpfung schwerer Kriminalität und der Abwehr schwerer Bedrohungen der öffentlichen Sicherheit gespeichert wurden, und zum anderen, nach der Erlangung dieses Zugangs, die Nutzung der Daten zur Untersuchung von Dienstvergehen im Zusammenhang mit Korruption.

24 Aus der Rechtsprechung des Gerichtshofs, insbesondere aus dem Urteil vom 6. Oktober 2020, Privacy International (C-623/17, EU:C:2020:790, Rn. 39), gehe zum einen hervor, dass Art. 15 Abs. 1 der Richtlinie 2002/58 in Verbindung mit ihrem Art. 3 dahin auszulegen sei, dass in den Geltungsbereich der Richtlinie nicht nur eine Rechtsvorschrift falle, die den Betreibern elektronischer Kommunikationsdienste vorschreibe, Verkehrs- und Standortdaten auf Vorrat zu speichern, sondern auch eine Rechtsvorschrift, die sie verpflichte, den zuständigen nationalen Behörden Zugang zu diesen Daten zu gewähren. Zum anderen ergebe sich aus dieser Rechtsprechung, insbesondere aus dem Urteil vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152, Rn. 33 und 35), dass in Bezug auf das Ziel der Verhütung,

Ermittlung, Feststellung und Verfolgung von Straftaten nach dem Grundsatz der Verhältnismäßigkeit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit schwerwiegende Eingriffe in die in den Art. 7 und 8 der Charta verankerten Grundrechte rechtfertigen könnten. wie sie mit der Speicherung von Verkehrs- und Standortdaten, sei sie allgemein und unterschiedslos oder zielgerichtet, verbunden seien.

25 Der Gerichtshof habe sich jedoch noch nicht zu den Auswirkungen der späteren Nutzung der fraglichen Daten auf den Eingriff in die Grundrechte geäußert. Dabei sei fraglich, ob auch eine derartige spätere Nutzung als Eingriff von solcher Schwere in die in den Art. 7 und 8 der Charta verankerten Grundrechte anzusehen sei, dass er nur zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit gerechtfertigt sein könne, was die Möglichkeit ausschließen würde, diese Daten bei Untersuchungen wegen Dienstvergehen im Zusammenhang mit Korruption zu nutzen.

26 Unter diesen Umständen hat der Lietuvos vyriausiasis administracinis teismas (Oberstes Verwaltungsgericht von Litauen) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Frage zur Vorabentscheidung vorzulegen:

Ist Art. 15 Abs. 1 der Richtlinie 2002/58 in Verbindung mit den Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta dahin auszulegen, dass es den zuständigen Behörden untersagt ist, von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherte Daten, die Informationen über die Daten und die Kommunikationen eines Nutzers eines elektronischen Kommunikationsmittels liefern können, im Rahmen von Ermittlungen wegen Dienstvergehen im Zusammenhang mit Korruption zu nutzen, unabhängig davon, ob der Zugang zu diesen Daten im konkreten Fall zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit gewährt wurde?

Zur Vorlagefrage

27 Mit seiner Frage möchte das vorlegende Gericht im Wesentlichen wissen, 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 dem entgegensteht, dass personenbezogene Daten elektronischer Kommunikationsvorgänge, die in Anwendung einer aufgrund dieser Bestimmung erlassenen Rechtsvorschrift von Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert und in der Folge in Anwendung dieser Rechtsvorschrift den zuständigen Behörden zur Bekämpfung schwerer Kriminalität zur Verfügung gestellt

wurden, im Rahmen von Untersuchungen wegen Dienstvergehen im Zusammenhang mit Korruption genutzt werden dürfen.

28 Vorab ist darauf hinzuweisen, dass nach den Angaben in der Vorlageentscheidung die Verwaltungsakte des Verfahrens, das zu den im Ausgangsverfahren in Rede stehenden Anordnungen (siehe oben, Rn. 19) geführt hat, zwar auch Informationen enthielt, die von den zuständigen Behörden dank der durch zwei gerichtliche Beschlüsse zu Zwecken der Strafverfolgung genehmigten Überwachung und Aufzeichnung elektronischer Kommunikationen gesammelt wurden; das vorlegende Gericht wirft jedoch nicht die Frage nach der Nutzung personenbezogener Daten, die ohne Zutun der Betreiber elektronischer Kommunikationsdienste erlangt wurden, auf, sondern die Frage nach der späteren Nutzung personenbezogener Daten, die von solchen Betreibern auf der Grundlage einer Rechtsvorschrift des Mitgliedstaats, mit der ihnen eine Aufbewahrungspflicht gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 auferlegt wurde, auf Vorrat gespeichert wurden.

29 Insoweit geht aus den Angaben im Vorabentscheidungsersuchen hervor, dass die Daten, auf die sich die Vorlagefrage bezieht, gemäß Art. 65 Abs. 2 des Gesetzes über die elektronische Kommunikation in Verbindung mit dessen Anhang 1 gespeichert wurden, wonach die Betreiber elektronischer Kommunikationsdienste verpflichtet sind, Verkehrs- und Standortdaten im Zusammenhang mit solchen Kommunikationen zur Bekämpfung schwerer Kriminalität allgemein und unterschiedslos auf Vorrat zu speichern.

30 Hinsichtlich der Voraussetzungen, unter denen diese Daten in einem Verwaltungsverfahren wegen Dienstvergehen im Zusammenhang mit Korruption genutzt werden dürfen, ist zunächst darauf hinzuweisen, dass ein Zugang zu ihnen in Anwendung einer gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassenen Rechtsvorschrift nur gewährt werden darf, wenn sie von den Betreibern in einer mit dieser Bestimmung im Einklang stehenden Weise gespeichert wurden (vgl. in diesem Sinne Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 29 und die dort angeführte Rechtsprechung). Sodann ist eine spätere Nutzung von Verkehrs- und Standortdaten im Zusammenhang mit solchen Kommunikationen zur Bekämpfung schwerer Kriminalität nur möglich, wenn die Vorratsspeicherung dieser Daten durch die Betreiber elektronischer Kommunikationsdienste im Einklang mit Art. 15 Abs. 1 der Richtlinie 2002/58 in seiner Auslegung durch die Rechtsprechung des Gerichtshofs stand und wenn der den zuständigen Behörden gewährte Zugang zu ihnen ebenfalls mit dieser Bestimmung im Einklang stand.

31 Insoweit hat der Gerichtshof bereits entschieden, 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 Rechtsvorschriften entgegensteht, die präventiv zur Bekämpfung

schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen (Urteil vom 20. September 2022, SpaceNet und Telekom Deutschland, C-793/19 und C-794/19, EU:C:2022:702, Rn. 74 und 131 sowie die dort angeführte Rechtsprechung). Dagegen steht Art. 15 Abs. 1 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta Rechtsvorschriften nicht entgegen, die zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit

– auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen,

– für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen,

– eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen und

– vorsehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben werden kann, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern,

sofern diese Rechtsvorschriften durch klare und präzise Regeln sicherstellen, dass bei der Vorratsspeicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen (Urteil vom 20. September 2022, SpaceNet und Telekom Deutschland, C-793/19 und C-794/19, EU:C:2022:702, Rn. 75 und die dort angeführte Rechtsprechung).

32 Zu den Zielen, die eine Nutzung der von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten durch Behörden in Anwendung einer mit diesen Bestimmungen im Einklang stehenden Rechtsvorschrift rechtfertigen können, ist darauf hinzuweisen, dass Art. 15 Abs. 1 der Richtlinie 2002/58 es den Mitgliedstaaten gestattet, Ausnahmen von der in Art. 5 Abs. 1 der Richtlinie aufgestellten grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit personenbezogener Daten sowie den entsprechenden, u. a. in den Art. 6 und 9 der Richtlinie genannten Pflichten zu

schaffen, sofern eine solche Beschränkung für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs elektronischer Kommunikationssysteme in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten u. a. durch Rechtsvorschriften vorsehen, dass Daten aus einem dieser Gründe für begrenzte Zeit aufbewahrt werden (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 110).

33 Art. 15 Abs. 1 der Richtlinie 2002/58 vermag es aber nicht zu rechtfertigen, dass die Ausnahme von der grundsätzlichen Verpflichtung, die Vertraulichkeit der elektronischen Kommunikation und der damit verbundenen Daten sicherzustellen, und insbesondere von dem in Art. 5 der Richtlinie vorgesehenen Verbot, diese Daten zu speichern, zur Regel wird, soll die letztgenannte Vorschrift nicht weitgehend ausgehöhlt werden (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 40).

34 Hinsichtlich der Ziele, die eine Beschränkung der insbesondere in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten rechtfertigen können, hat der Gerichtshof bereits entschieden, dass die Aufzählung der in ihrem Art. 15 Abs. 1 Satz 1 genannten Ziele abschließend ist, so dass eine aufgrund dieser Bestimmung erlassene Rechtsvorschrift tatsächlich strikt einem von ihnen dienen muss (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 41).

35 Was die dem Gemeinwohl dienenden Ziele anbelangt, die eine nach Art. 15 Abs. 1 der Richtlinie 2002/58 erlassene Vorschrift rechtfertigen können, geht aus der Rechtsprechung des Gerichtshofs hervor, dass nach dem Grundsatz der Verhältnismäßigkeit eine Hierarchie zwischen diesen Zielen entsprechend ihrer jeweiligen Bedeutung besteht und dass die Bedeutung des mit einer solchen Vorschrift verfolgten Ziels im Verhältnis zur Schwere des daraus resultierenden Eingriffs stehen muss (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 56).

36 Insoweit übersteigt die Bedeutung des Ziels des Schutzes der nationalen Sicherheit im Licht von Art. 4 Abs. 2 EUV, wonach der Schutz der nationalen Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt, die der übrigen von Art. 15 Abs. 1 der Richtlinie 2002/58 erfassten Ziele, insbesondere der Ziele, die Kriminalität im Allgemeinen, auch schwere Kriminalität, zu bekämpfen und die öffentliche Sicherheit zu schützen. Vorbehaltlich der Erfüllung der übrigen Anforderungen von Art. 52 Abs. 1 der Charta ist das Ziel, die nationale Sicherheit zu wahren, daher geeignet, Maßnahmen zu rechtfertigen, die schwerere Grundrechtseingriffe enthalten als solche, die mit den übrigen Zielen gerechtfertigt werden könnten (Urteil vom

5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 57 und die dort angeführte Rechtsprechung).

37 Zum Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten hat der Gerichtshof festgestellt, dass im Einklang mit dem Grundsatz der Verhältnismäßigkeit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet sind, die mit der Speicherung von Verkehrs- und Standortdaten verbundenen schweren Eingriffe in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, zu rechtfertigen. Daher können nur Eingriffe in die genannten Grundrechte, die nicht schwer sind, durch das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 59 und die dort angeführte Rechtsprechung).

38 Nach dieser Rechtsprechung sind zwar die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit in der Hierarchie der dem Gemeinwohl dienenden Ziele von geringerer Bedeutung als der Schutz der nationalen Sicherheit (vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 99), doch übersteigt ihre Bedeutung die der Bekämpfung von Straftaten im Allgemeinen und der Verhütung leichter Bedrohungen der öffentlichen Sicherheit.

39 In diesem Kontext ist allerdings darauf hinzuweisen (siehe auch oben, Rn. 31), dass die Möglichkeit für die Mitgliedstaaten, eine Beschränkung u. a. der in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten zu rechtfertigen, zu beurteilen ist, indem die Schwere des mit einer solchen Beschränkung verbundenen Eingriffs bestimmt und geprüft wird, ob das mit ihr verfolgte dem Gemeinwohl dienende Ziel in angemessenem Verhältnis zur Schwere des Eingriffs steht (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 131).

40 Außerdem hat der Gerichtshof bereits entschieden, dass der Zugang zu den von Betreibern in Anwendung einer gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassenen Rechtsvorschrift auf Vorrat gespeicherten Verkehrs- und Standortdaten, der unter vollständiger Beachtung der sich aus der Rechtsprechung zur Auslegung dieser Richtlinie ergebenden Voraussetzungen zu erfolgen hat, grundsätzlich nur mit dem dem Gemeinwohl dienenden Ziel gerechtfertigt werden kann, zu dem die Speicherung den Betreibern auferlegt wurde. Etwas anderes gilt nur, wenn die Bedeutung des mit dem Zugang verfolgten Ziels die Bedeutung des Ziels, das die Speicherung gerechtfertigt hat, übersteigt (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 98 und die dort angeführte Rechtsprechung).

41 Diese Erwägungen gelten entsprechend für eine spätere Nutzung der Verkehrs- und Standortdaten, die von Betreibern elektronischer Kommunikationsdienste in Anwendung einer nach Art. 15 Abs. 1 der Richtlinie 2002/58 zur Bekämpfung schwerer Kriminalität erlassenen Rechtsvorschrift auf Vorrat gespeichert wurden. Solche Daten dürfen nämlich, nachdem sie gespeichert und den zuständigen Behörden zum Zweck der Bekämpfung schwerer Kriminalität zur Verfügung gestellt wurden, nicht an andere Behörden übermittelt und genutzt werden, um Ziele wie im vorliegenden Fall die Bekämpfung von Dienstvergehen im Zusammenhang mit Korruption zu erreichen, die in der Hierarchie der dem Gemeinwohl dienenden Ziele von geringerer Bedeutung sind als die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit. Die Gewährung von Zugang zu den auf Vorrat gespeicherten Daten und ihre Nutzung würden in einer solchen Situation nämlich der oben in den Rn. 33, 35 bis 37 und 40 angesprochenen Hierarchie der dem Gemeinwohl dienenden Ziele zuwiderlaufen (vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 99).

42 Zu dem von der tschechischen Regierung und von Irland in ihren schriftlichen Erklärungen vorgebrachten Argument, ein Disziplinarverfahren wegen Dienstvergehen im Zusammenhang mit Korruption könne den Schutz der öffentlichen Sicherheit betreffen, genügt der Hinweis, dass das vorlegende Gericht in seiner Vorlageentscheidung keine schwere Bedrohung der öffentlichen Sicherheit angeführt hat.

43 Überdies trifft es zwar zu, dass Verwaltungsuntersuchungen wegen Disziplinar- oder Dienstvergehen im Zusammenhang mit Korruption eine wichtige Rolle bei der Bekämpfung solcher Handlungen spielen können, doch dient eine Rechtsvorschrift, die solche Untersuchungen vorsieht, nicht tatsächlich und strikt dem Ziel der Verfolgung und Ahndung von Straftaten im Sinne von Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58, der nur die Strafverfolgung betrifft.

44 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 dem entgegensteht, dass personenbezogene Daten elektronischer Kommunikationsvorgänge, die in Anwendung einer aufgrund dieser Bestimmung erlassenen Rechtsvorschrift von Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert und in der Folge in Anwendung dieser Rechtsvorschrift den zuständigen Behörden zur Bekämpfung schwerer Kriminalität zur Verfügung gestellt wurden, im Rahmen von Untersuchungen wegen Dienstvergehen im Zusammenhang mit Korruption genutzt werden dürfen.

Kosten

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

Aus diesen Gründen hat der Gerichtshof (Erste 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 dem entgegensteht, dass personenbezogene Daten elektronischer Kommunikationsvorgänge, die in Anwendung einer aufgrund dieser Bestimmung erlassenen Rechtsvorschrift von Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert und in der Folge in Anwendung dieser Rechtsvorschrift den zuständigen Behörden zur Bekämpfung schwerer Kriminalität zur Verfügung gestellt wurden, im Rahmen von Untersuchungen wegen Dienstvergehen im Zusammenhang mit Korruption genutzt werden dürfen.