Sammlung der Rechtsprechung

URTEIL DES GERICHTSHOFS (Große Kammer)

2. März 2021 *

„Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten in der elektronischen Kommunikation – Richtlinie 2002/58/EG – Betreiber elektronischer Kommunikationsdienste – Vertraulichkeit der Kommunikation – Beschränkungen – Art. 15 Abs. 1 – Art. 7, 8 und 11 sowie Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union – Rechtsvorschriften, die eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten durch die Betreiber elektronischer Kommunikationsdienste vorsehen – Zugang der nationalen Behörden zu den zu Ermittlungszwecken gespeicherten Daten – Bekämpfung der Kriminalität im Allgemeinen – Genehmigung der Staatsanwaltschaft – Nutzung der Daten als Beweise im Rahmen des Strafprozesses – Zulässigkeit“

In der Rechtssache C-746/18

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Riigikohus (Oberster Gerichtshof, Estland) mit Entscheidung vom 12. November 2018, beim Gerichtshof eingegangen am 29. November 2018, in dem Strafverfahren gegen

H. K.,

Beteiligte:

Prokuratuur,

erlässt

DER GERICHTSHOF (Große Kammer)

unter Mitwirkung des Präsidenten K. Lenaerts, der Vizepräsidentin R. Silva de Lapuerta, der Kammerpräsidenten J.-C. Bonichot und A. Arabadjiev, der Kammerpräsidentin A. Prechal, des Kammerpräsidenten L. Bay Larsen, der Richter T. von Danwitz (Berichterstatter) und M. Safjan, der Richterin K. Jürimäe sowie der Richter C. Lycourgos und P. G. Xuereb,

Generalanwalt: G. Pitruzzella,

Kanzler: C. Strömholm, Verwaltungsrätin,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 15. Oktober 2019,

unter Berücksichtigung der Erklärungen

– von H. K., vertreten durch S. Reinsaar, vandeadvokaat,

* Verfahrenssprache: Estnisch.

– der Prokuratuur, vertreten durch T. Pern und M. Voogma als Bevollmächtigte,

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

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

– Irlands, vertreten durch M. Browne, G. Hodge J. Quaney und A. Joyce als Bevollmächtigte im Beistand von D. Fennelly, Barrister,

– der französischen Regierung, zunächst vertreten durch D. Dubois, D. Colas, E. de Moustier und A.-L. Desjonquères, dann durch D. Dubois, E. de Moustier und A.-L. Desjonquères als Bevollmächtigte,

– der lettischen Regierung, zunächst vertreten durch V. Kalniņa und I. Kucina, dann durch V. Soņeca und V. Kalniņa als Bevollmächtigte,

– der ungarischen Regierung, vertreten durch M. Z. Fehér und A. Pokoraczki als Bevollmächtigte,

– der polnischen Regierung, vertreten durch B. Majczyna als Bevollmächtigten,

– der portugiesischen Regierung, vertreten durch L. Inez Fernandes, P. Barros da Costa, L. Medeiros und I. Oliveira als Bevollmächtigte,

– der finnischen Regierung, vertreten durch J. Heliskoski als Bevollmächtigten,

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

– der Europäischen Kommission, zunächst vertreten durch H. Kranenborg, M. Wasmeier, P. Costa de Oliveira und K. Toomus, dann durch H. Kranenborg, M. Wasmeier und E. Randvere als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 21. Januar 2020

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 Es ergeht im Rahmen eines Strafverfahrens gegen H. K. wegen Diebstahls, Verwendung der Bankkarte eines Dritten und Gewalttaten gegenüber Beteiligten an einem Gerichtsverfahren.

Rechtlicher Rahmen

Unionsrecht

3 In den Erwägungsgründen 2 und 11 der Richtlinie 2002/58 wird ausgeführt:

„(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 [Unionsrecht] 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 sieht vor:

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

„(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. 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“) der Richtlinie 2002/58 sieht in Abs. 1 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 Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) 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] 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 [Unionsrechts] einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.“

Estnisches Recht

Gesetz über die elektronische Kommunikation

9 Das Elektroonilise side seadus (Gesetz über die elektronische Kommunikation, RT I 2004, 87, 593) bestimmt in der im Ausgangsverfahren anwendbaren Fassung (im Folgenden: Gesetz über die elektronische Kommunikation) in § 111[1] („Pflicht zur Vorratsspeicherung von Daten“):

„…

(2) Anbieter von Telefon- und Mobiltelefondiensten sowie Telefonnetz- und Mobiltelefonnetzdiensten sind verpflichtet, folgende Daten auf Vorrat zu speichern:

1. Nummer des anrufenden Anschlusses sowie Name und Anschrift des Teilnehmers;

2. Nummer des angerufenen Anschlusses sowie Name und Anschrift des Teilnehmers;

3. bei der Nutzung eines Zusatzdienstes wie einer Rufweiterleitung oder einer Rufumleitung die gewählte Nummer sowie Name und Anschrift des Teilnehmers;

4. Datum und Uhrzeit des Beginns und des Endes eines Anrufs;

5. der in Anspruch genommene Telefon- oder Mobiltelefondienst;

6. die Internationale Mobilfunk-Teilnehmerkennung (International Mobile Subscriber Identity – IMSI) des anrufenden und des angerufenen Anschlusses;

7. die Internationale Kennung der mobilen Endeinrichtung (International Mobile Equipment Identity – IMEI) des anrufenden und des angerufenen Anschlusses;

8. die Standortkennung bei Beginn des Anrufs;

9. Daten zur geografischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung während des Zeitraums, in dem die Daten auf Vorrat gespeichert werden;

10. im Fall eines vorbezahlten anonymen Mobiltelefondienstes Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts, an dem der Dienst aktiviert wurde;

…

(4) Die in den Abs. 2 und 3 dieses Paragrafen genannten Daten werden für einen Zeitraum von einem Jahr ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert, wenn diese Daten im Zuge der Bereitstellung eines Kommunikationsdienstes erzeugt oder verarbeitet wurden …

…

(11) Die in den Abs. 2 und 3 dieses Paragrafen genannten Daten werden weitergeleitet

1. gemäß dem Kriminaalmenetluse seadustik [(Strafprozessordnung)] an eine Ermittlungsbehörde, eine zu Überwachungsmaßnahmen ermächtigte Stelle, die Staatsanwaltschaft und das Gericht;

…“

Strafprozessordnung

10 § 17 der Strafprozessordnung bestimmt:

„(1) Beteiligte des Gerichtsverfahrens sind: die Staatsanwaltschaft, …

…“

11 § 30 der Strafprozessordnung lautet:

„(1) Die Staatsanwaltschaft leitet das Ermittlungsverfahren, dessen Rechtmäßigkeit und Wirksamkeit sie gewährleistet, und vertritt die öffentliche Klage vor dem Gericht.

(2) Die Befugnisse der Staatsanwaltschaft im Strafverfahren werden im Namen der Staatsanwaltschaft von einem Staatsanwalt ausgeübt, der unabhängig handelt und nur an das Gesetz gebunden ist.“

12 § 90[1] der Strafprozessordnung sieht vor:

„…

(2) Die Ermittlungsbehörde kann im Ermittlungsverfahren mit Genehmigung der Staatsanwaltschaft oder im gerichtlichen Verfahren mit Genehmigung des Gerichts von einem Anbieter elektronischer Kommunikationsdienste die in § 111[1] Abs. 2 und 3 des Gesetzes über die elektronische Kommunikation aufgezählten Daten anfordern, die in Abs. 1 des vorliegenden Paragrafen nicht genannt sind. In der Genehmigung der Anforderung wird der Zeitraum, für den die Anforderung der Daten genehmigt wird, genau angegeben.

(3) Gemäß dem vorliegenden Paragrafen dürfen Daten nur angefordert werden, wenn dies unerlässlich ist, um das Ziel des Strafverfahrens zu erreichen."

13 § 211 der Strafprozessordnung lautet:

„(1) Ziel des Ermittlungsverfahrens ist es, Beweise zu erheben und die übrigen Voraussetzungen für ein gerichtliches Verfahren zu schaffen.

(2) Im Ermittlungsverfahren klären die Ermittlungsbehörde und die Staatsanwaltschaft die den Beschuldigten oder Angeklagten entlastenden und belastenden Umstände auf."

Gesetz über die Staatsanwaltschaft

14 Das Prokuratuuriseadus (Gesetz über die Staatsanwaltschaft, RT I 1998, 41, 625) bestimmt in der im Ausgangsverfahren anwendbaren Fassung in § 1:

„(1) Die Staatsanwaltschaft ist eine dem Zuständigkeitsbereich des Justizministeriums unterstehende Behörde, die an der Planung der zur Bekämpfung und Aufklärung von Straftaten notwendigen Überwachungsmaßnahmen beteiligt ist, das Ermittlungsverfahren leitet, dessen Rechtmäßigkeit und Wirksamkeit gewährleistet, die öffentliche Klage vor dem Gericht vertritt und sonstige ihr durch Gesetz übertragene Aufgaben wahrnimmt.

(2) Die Staatsanwaltschaft ist bei der Erfüllung ihrer gesetzlichen Aufgaben unabhängig und handelt gemäß dem vorliegenden Gesetz, sonstigen Gesetzen und auf der Grundlage dieser Gesetze erlassener Rechtsakte.

…"

15 § 2 Abs. 2 dieses Gesetzes bestimmt:

„Der Staatsanwalt ist bei der Erfüllung seiner Aufgaben unabhängig und handelt ausschließlich nach dem Gesetz und seiner Überzeugung."

Ausgangsverfahren und Vorlagefragen

16 Mit Urteil vom 6. April 2017 wurde H. K. vom Viru Maakohus (Gericht erster Instanz Viru, Estland) wegen mehrerer zwischen dem 17. Januar 2015 und dem 1. Februar 2016 begangener Diebstähle materieller Güter (im Wert von drei bis 40 Euro) sowie von Geldbeträgen (zwischen 5,20 Euro und 2 100 Euro), wegen Nutzung der Bankkarte eines Dritten, wodurch diesem ein Schaden in Höhe von 3 941,82 Euro entstand, und wegen Gewalttaten gegenüber Beteiligten an einem sie betreffenden Gerichtsverfahren zu einer Freiheitsstrafe von zwei Jahren verurteilt.

17 Bei der Verurteilung von H. K. wegen dieser Straftaten stützte sich der Viru Maakohus (Gericht erster Instanz Viru) u. a. auf mehrere Protokolle, die anhand von Daten zu elektronischen Kommunikationen im Sinne von § 111[1] Abs. 2 des Gesetzes über die elektronische Kommunikation erstellt worden waren. Diese Daten hatte die Ermittlungsbehörde im Ermittlungsverfahren bei einem Anbieter elektronischer Telekommunikationsdienste erhoben, nachdem sie insoweit gemäß § 90[1] der Strafprozessordnung mehrere Genehmigungen der Viru Ringkonnaprokuratuur (Bezirksstaatsanwaltschaft Viru, Estland) eingeholt hatte. Diese am 28. Januar und 2. Februar 2015, am 2. November 2015 sowie am 25. Februar 2016 erteilten Genehmigungen betrafen mehrere Telefonnummern und verschiedene Internationale Mobilfunk-Teilnehmerkennungen von H. K. aus der Zeit vom 1. Januar bis 2. Februar 2015, vom 21. September 2015 sowie aus der Zeit vom 1. März 2015 bis 19. Februar 2016.

18 Die von H. K. gegen das Urteil des Viru Maakohus (Gericht erster Instanz Viru) eingelegte Berufung wurde vom Tartu Ringkonnakohus (Bezirksgericht Tartu, Estland) mit Urteil vom 17. November 2017 zurückgewiesen.

19 H. K. legte dagegen Kassationsbeschwerde beim Riigikohus (Oberster Gerichtshof, Estland) ein, wobei sie u. a. die Unzulässigkeit der Protokolle rügte, die anhand der vom Anbieter elektronischer Kommunikationsdienste erlangten Daten erstellt worden waren. Sie machte geltend, wie dem Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, im Folgenden: Urteil Tele2, EU:C:2016:970), zu entnehmen sei, verstießen die Bestimmungen von § 111[1] des Gesetzes über die elektronische Kommunikation, wonach die Diensteanbieter verpflichtet seien, Daten über Kommunikationen auf Vorrat zu speichern, sowie die Verwendung dieser Daten zu ihrer Verurteilung im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta gegen Art. 15 Abs. 1 der Richtlinie 2002/58.

20 Das vorlegende Gericht führt aus, es sei fraglich, ob die anhand von Daten im Sinne von § 111[1] Abs. 2 des Gesetzes über die elektronische Kommunikation erstellten Protokolle als zulässige Beweise angesehen werden könnten. Die Zulässigkeit der im Ausgangsverfahren in Rede stehenden Protokolle als Beweise hänge davon ab, inwieweit die Erhebung der Daten, anhand deren die Protokolle erstellt worden seien, mit Art. 15 Abs. 1 der Richtlinie 2002/58, ausgelegt im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta, im Einklang stehe.

21 Zur Beantwortung dieser Frage müsse geklärt werden, ob Art. 15 Abs. 1 im Licht der Charta dahin auszulegen sei, dass der Zugang der nationalen Behörden zu Daten, die es ermöglichten, die Quelle und den Adressaten einer Telefon- oder Mobiltelefonkommunikation eines Verdächtigen, Datum, Uhrzeit, Dauer und Art dieser Kommunikation sowie das verwendete Kommunikationsmaterial und den Standort des verwendeten mobilen Geräts zu bestimmen, einen so schweren Eingriff in die fraglichen Grundrechte darstelle, dass der Zugang auf die Bekämpfung schwerer Kriminalität beschränkt werden müsse, unabhängig davon, für welchen Zeitraum die nationalen Behörden Zugang zu den auf Vorrat gespeicherten Daten begehrt hätten.

22 Die Länge dieses Zeitraums sei jedoch ein wesentlicher Gesichtspunkt für die Beurteilung der Schwere des Eingriffs in Form des Zugangs zu den Verkehrs- und Standortdaten. Wenn dieser Zeitraum sehr kurz oder die Menge der gesammelten Daten sehr begrenzt sei, stelle sich die Frage, ob das Ziel der Bekämpfung der Kriminalität im Allgemeinen und nicht nur der Bekämpfung schwerer Kriminalität einen solchen Eingriff rechtfertigen könne.

23 Schließlich bestünden Zweifel, ob die estnische Staatsanwaltschaft als unabhängige Verwaltungsbehörde im Sinne von Rn. 120 des Urteils vom 21. Dezember 2016, Tele2 (C-203/15 und C-698/15, EU:C:2016:970), angesehen werden könne, die befugt sei, den Zugang der Ermittlungsbehörde zu Daten über elektronische Kommunikationen wie den von § 111[1] Abs. 2 des Gesetzes über die elektronische Kommunikation erfassten zu genehmigen.

24 Die Staatsanwaltschaft leite das Ermittlungsverfahren und gewährleiste dessen Rechtmäßigkeit und Wirksamkeit. Das Ziel dieses Verfahrens bestehe insbesondere darin, Beweise zu erheben, wobei die Ermittlungsbehörde und die Staatsanwaltschaft bei jedem Angeklagten oder Beschuldigten die entlastenden und belastenden Umstände prüften. Wenn die Staatsanwaltschaft der Überzeugung sei, dass alle erforderlichen Beweise gesammelt worden seien, vertrete sie die öffentliche Klage gegen den Beschuldigten. Die Befugnisse der Staatsanwaltschaft würden in deren Namen von einem Staatsanwalt ausgeübt, der bei der Erfüllung seiner Aufgaben unabhängig sei, wie sich aus § 30 Abs. 1 und 2 der Strafprozessordnung sowie aus den § 1 und 2 des Gesetzes über die Staatsanwaltschaft ergebe.

25 In diesem Kontext fügt das vorlegende Gericht hinzu, seine Zweifel an der unionsrechtlich erforderlichen Unabhängigkeit beruhten vor allem darauf, dass die Staatsanwaltschaft nicht nur das Ermittlungsverfahren leite, sondern auch vor dem Gericht die öffentliche Klage vertrete, so dass sie nach nationalem Recht Beteiligte des Strafverfahrens sei.

26 Unter diesen Umständen hat der Riigikohus (Oberster Gerichtshof) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Ist Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen, dass in einem Strafverfahren der Zugang nationaler Behörden zu Daten, die es ermöglichen, die Quelle und den Adressaten, das Datum, die Uhrzeit und die Dauer, die Art des Kommunikationsdiensts, die verwendete Endeinrichtung sowie den Standort des verwendeten mobilen Geräts in Bezug auf eine Telefon- oder Mobiltelefonkommunikation eines Beschuldigten festzustellen, einen so schweren Eingriff in die in den genannten Artikeln der Charta verankerten Grundrechte darstellt, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden muss, unabhängig davon, auf welchen Zeitraum sich die auf Vorrat gespeicherten Daten, zu denen die nationalen Behörden Zugang haben, beziehen?

2. Ist Art. 15 Abs. 1 der Richtlinie 2002/58 ausgehend von dem in den Rn. 55 bis 57 des Urteils vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, Rn. 55 bis 57), zum Ausdruck gebrachten Grundsatz der Verhältnismäßigkeit dahin auszulegen, dass, wenn die Menge der in der ersten Frage genannten Daten, zu denen die staatlichen Behörden Zugang haben (sowohl nach der Art der Daten als auch nach ihrem zeitlichen Ausmaß), nicht groß ist, der damit einhergehende Grundrechtseingriff durch den Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein kann und dass die Straftaten, die durch den Eingriff bekämpft werden sollen, umso schwerer sein müssen, je größer die Menge der Daten ist, zu denen die staatlichen Behörden Zugang haben?

3. Bedeutet die in Nr. 2 des Tenors des Urteils vom 21. Dezember 2016, Tele2 (C-203/15 und C-698/15, EU:C:2016:970), genannte Anforderung, dass der Datenzugang der zuständigen staatlichen Behörden einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde unterliegen muss, dass Art. 15 Abs. 1 der Richtlinie 2002/58 dahin auszulegen ist, dass die Staatsanwaltschaft, die das Ermittlungsverfahren leitet, wobei sie nach dem Gesetz zu unabhängigem Handeln verpflichtet ist und nur an das Gesetz gebunden ist und im Ermittlungsverfahren sowohl die den Angeklagten belastenden als auch die ihn entlastenden Umstände aufklärt, aber später im gerichtlichen Verfahren die öffentliche Klage vertritt, als unabhängige Verwaltungsbehörde angesehen werden kann?

Zu den Vorlagefragen

Zur ersten und zur zweiten Frage

27 Mit der ersten und der zweiten Vorlagefrage, die gemeinsam zu prüfen sind, möchte das vorlegende Gericht 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 einer nationalen Regelung entgegensteht, die es den Behörden zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten ermöglicht, Zugang zu einem Satz von Verkehrs- oder Standortdaten zu erlangen, die geeignet sind, Informationen über die von einem Nutzer eines elektronischen Kommunikationsmittels getätigten Kommunikationen oder über den Standort der von ihm verwendeten Endgeräte zu liefern und genaue Schlüsse auf sein Privatleben zuzulassen, ohne dass sich dieser Zugang auf Verfahren zur Bekämpfung schwerer Kriminalität beschränken würde, und ob dies unabhängig davon gilt, für welchen Zeitraum der Zugang zu den betreffenden Daten begehrt wird und welche Menge und Art von Daten für einen solchen Zeitraum verfügbar ist.

28 Insoweit ergibt sich aus den in der Vorlageentscheidung enthaltenen und von der estnischen Regierung in der mündlichen Verhandlung bestätigten Angaben, dass die Daten, zu denen die nationale Ermittlungsbehörde im Ausgangsverfahren Zugang hatte, gemäß § 111[1] Abs. 2 und 4 des Gesetzes über die elektronische Kommunikation gesammelt wurden, der die Betreiber elektronischer Kommunikationsdienste dazu verpflichtet, die Verkehrs- und Standortdaten in Bezug auf Telefonie und Mobiltelefonie ein Jahr lang allgemein und unterschiedslos auf Vorrat zu speichern. Diese Daten ermöglichen es u. a., die Quelle und den Adressaten einer Telefon- oder Mobiltelefonkommunikation einer Person zu rekonstruieren und zu identifizieren, Datum, Uhrzeit, Dauer und Art dieser Kommunikation zu ermitteln, das verwendete Kommunikationsmaterial zu identifizieren und den Standort des Mobiltelefons zu bestimmen, ohne dass eine Nachricht zwangsläufig weitergeleitet wurde. Außerdem bieten sie die Möglichkeit, die Häufigkeit der Kommunikationen des Nutzers mit bestimmten Personen während eines konkreten Zeitraums zu ermitteln. Überdies kann, wie die estnische Regierung in der mündlichen Verhandlung bestätigt hat, der Zugang zu den genannten Daten im Bereich der Kriminalitätsbekämpfung für Straftaten jeder Art beantragt werden.

29 Zu den Voraussetzungen, unter denen Behörden in Anwendung einer gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 getroffenen Maßnahme zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten Zugang zu den von den Betreibern elektronischer Kommunikationsdienste gespeicherten Verkehrs- und Standortdaten gewährt 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 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 167).

30 Insoweit hat der Gerichtshof ferner entschieden, dass 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 (vgl. in diesem Sinne 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. 168).

31 Zu den Zielen, die einen Zugang der Behörden zu Daten, die von den Betreibern elektronischer Kommunikationsdienste in Anwendung einer mit diesen Bestimmungen im Einklang stehenden Maßnahme auf Vorrat gespeichert wurden, rechtfertigen können, ergibt sich zum einen aus der Rechtsprechung des Gerichtshofs, dass ein solcher Zugang nur mit dem dem Gemeinwohl dienenden Ziel gerechtfertigt werden kann, zu dem die Speicherung den Betreibern auferlegt wurde (vgl. in diesem Sinne 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. 166).

32 Zum anderen hat der Gerichtshof entschieden, dass die Möglichkeit für die Mitgliedstaaten, eine Beschränkung der u. a. 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 die mit ihr verfolgte, dem Gemeinwohl dienende Zielsetzung 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 und die dort angeführte Rechtsprechung).

33 Was das mit der im Ausgangsverfahren in Rede stehenden Regelung verfolgte Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten anbelangt, sind im Einklang mit dem Grundsatz der Verhältnismäßigkeit nur die Bekämpfung schwerer Kriminalität und die Verhütung ernster Bedrohungen der öffentlichen Sicherheit geeignet, die mit der Speicherung von Verkehrs- und Standortdaten – unabhängig davon, ob sie allgemein und unterschiedslos oder gezielt erfolgt – 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 als schwerwiegend zu charakterisieren sind, durch das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt werden, das mit der im Ausgangsverfahren in Rede stehenden Regelung verfolgt wird (vgl. in diesem Sinne 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. 140 und 146).

34 Insoweit ist u. a. entschieden worden, dass Rechtsvorschriften, die auf die Verarbeitung von die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten als solchen, insbesondere auf ihre Speicherung und den Zugang zu ihnen, zum alleinigen Zweck der Identifizierung des betreffenden Nutzers abzielen, ohne dass die Daten mit Informationen über die erfolgten Kommunikationen in Verbindung gebracht werden können, durch den in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 genannten Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein können. Diese Daten ermöglichen es nämlich für sich genommen weder, das Datum, die Uhrzeit, die Dauer und die Adressaten der Kommunikationen in Erfahrung zu bringen, noch die Orte, an denen sie stattfanden, oder wie häufig dies mit bestimmten Personen innerhalb eines gegebenen Zeitraums geschah, so dass sie, abgesehen von Kontaktdaten der Nutzer elektronischer Kommunikationsmittel wie ihren Adressen, keine Informationen über die konkreten Kommunikationen und infolgedessen über ihr Privatleben liefern. Der Eingriff, der mit einer auf diese Daten abzielenden Maßnahme verbunden ist, kann somit grundsätzlich nicht als schwer eingestuft werden (vgl. in diesem Sinne 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. 157 und 158 sowie die dort angeführte Rechtsprechung).

35 Unter diesen Umständen können nur die Ziele der Bekämpfung schwerer Kriminalität oder der Verhütung ernster Bedrohungen der öffentlichen Sicherheit den Zugang der Behörden zu einem Satz von Verkehrs- oder Standortdaten rechtfertigen, die geeignet sind, Informationen über die Kommunikationen 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 (vgl. in diesem Sinne Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 54), ohne dass andere die Verhältnismäßigkeit eines Zugangsantrags betreffende Faktoren wie die Länge des Zeitraums, für den der Zugang zu solchen Daten begehrt wird, dazu führen können, dass das Ziel, Straftaten im Allgemeinen zu verhüten, zu ermitteln, festzustellen und zu verfolgen, einen solchen Zugang zu rechtfertigen vermag.

36 Der Zugang zu einem Satz von Verkehrs- oder Standortdaten, wie sie gemäß § 111[1] des Gesetzes über die elektronische Kommunikation gespeichert werden, ist in der Tat geeignet, genaue oder sogar sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, zuzulassen, 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 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 117).

37 Dem vorlegenden Gericht ist zwar beizupflichten, dass die Menge der Daten, die von den Betreibern elektronischer Kommunikationsdienste in Bezug auf die elektronischen Kommunikationen, die Aufenthaltsorte und die Ortsveränderungen des Nutzers eines elektronischen Kommunikationsmittels gespeichert werden kann, grundsätzlich umso größer ist, je länger der Zeitraum ist, für den der Zugang zu solchen Daten begehrt wird, und es damit ermöglicht, anhand der konsultierten Daten eine größere Zahl von Schlüssen auf das Privatleben dieses Nutzers zu ziehen. Eine entsprechende Feststellung kann in Bezug auf die angeforderten Datenkategorien getroffen werden.

38 Um dem Erfordernis der Verhältnismäßigkeit zu genügen, wonach sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen (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. 130 und die dort angeführte Rechtsprechung), obliegt es daher den zuständigen nationalen Behörden, in jedem Einzelfall zu gewährleisten, dass sich sowohl die Kategorie oder Kategorien erfasster Daten als auch die Dauer, für die der Zugang zu ihnen begehrt wird, nach Maßgabe der konkreten Umstände auf das für die fraglichen Ermittlungen absolut Notwendige beschränken.

39 Der mit dem Zugang einer Behörde zu einem Satz von Verkehrs- oder Standortdaten, die Informationen über die Kommunikationen des Nutzers eines elektronischen Kommunikationsmittels oder über den Standort der von ihm verwendeten Endgeräte liefern können, verbundene Eingriff in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, ist in jedem Fall schwerwiegend, unabhängig von der Länge des Zeitraums, für den der Zugang zu den genannten Daten begehrt wird, und von der Menge oder Art der für einen solchen Zeitraum verfügbaren Daten, sofern der Datensatz, wie im Ausgangsverfahren, geeignet ist, genaue Schlüsse auf das Privatleben des oder der Betroffenen zuzulassen.

40 Insoweit kann selbst der Zugang zu einer begrenzten Menge von Verkehrs- oder Standortdaten oder der Zugang zu Daten für einen kurzen Zeitraum geeignet sein, genaue Informationen über das Privatleben des Nutzers eines elektronischen Kommunikationsmittels zu liefern. Außerdem sind die Menge der verfügbaren Daten und die daraus resultierenden konkreten Informationen über das Privatleben des Betroffenen Umstände, die erst nach Konsultation der fraglichen Daten beurteilt werden können. Die Zugangsgenehmigung wird aber vom Gericht oder von der zuständigen unabhängigen Stelle notwendigerweise erteilt, bevor die Daten und die daraus resultierenden Informationen konsultiert werden können. Somit erfolgt die Beurteilung der Schwere des in dem Zugang bestehenden Eingriffs notwendigerweise anhand der mit der angeforderten Kategorie von Daten allgemein verbundenen Gefahr für das Privatleben der Betroffenen, ohne dass es überdies darauf ankommt, ob die daraus resultierenden Informationen über das Privatleben im konkreten Fall sensiblen Charakter haben.

41 Schließlich ist in Anbetracht dessen, dass das vorlegende Gericht mit dem Antrag befasst ist, anhand von Verkehrs- und Standortdaten erstellte Protokolle für unzulässig zu erklären, weil die Bestimmungen von § 111[1] des Gesetzes über die elektronische Kommunikation sowohl in Bezug auf die Speicherung der Daten als auch in Bezug auf den Zugang zu ihnen gegen Art. 15 Abs. 1 der Richtlinie 2002/58 verstießen, darauf hinzuweisen, dass es beim gegenwärtigen Stand des Unionsrechts grundsätzlich allein Sache des nationalen Rechts ist, die Vorschriften für die Zulässigkeit und die Würdigung der durch eine unionsrechtswidrige allgemeine und unterschiedslose Speicherung dieser Daten erlangten Informationen und Beweise im Rahmen eines Strafverfahrens gegen Personen festzulegen, die im Verdacht stehen, Straftaten begangen zu haben (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. 222). Das Gleiche gilt für einen unionsrechtswidrigen Zugang nationaler Behörden zu den fraglichen Daten.

42 Nach ständiger Rechtsprechung ist es nämlich mangels einschlägiger unionsrechtlicher Vorschriften nach dem Grundsatz der Verfahrensautonomie Sache der innerstaatlichen Rechtsordnung jedes Mitgliedstaats, die Verfahrensmodalitäten für Klagen, die den Schutz der den Einzelnen aus dem Unionsrecht erwachsenden Rechte gewährleisten sollen, zu regeln, wobei sie jedoch nicht ungünstiger sein dürfen als diejenigen, die gleichartige, dem innerstaatlichen Recht unterliegende Sachverhalte regeln (Äquivalenzgrundsatz), und die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren dürfen (Effektivitätsgrundsatz) (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. 223 und die dort angeführte Rechtsprechung).

43 Zum Effektivitätsgrundsatz ist festzustellen, dass die nationalen Vorschriften über die Zulässigkeit und die Verwertung von Informationen und Beweisen darauf abzielen, nach Maßgabe der im nationalen Recht getroffenen Entscheidungen zu verhindern, dass einer Person, die im Verdacht steht, Straftaten begangen zu haben, durch rechtswidrig erlangte Informationen und Beweise unangemessene Nachteile entstehen. Dieses Ziel kann aber im nationalen Recht nicht nur durch ein Verbot der Verwertung solcher Informationen und Beweise erreicht werden, sondern auch durch nationale Vorschriften und Praktiken für die Würdigung und Gewichtung der Informationen und Beweise oder durch eine Berücksichtigung ihrer Rechtswidrigkeit im Rahmen der Strafzumessung (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. 225).

44 Ob es erforderlich ist, Informationen und Beweise auszuschließen, die unter Verstoß gegen unionsrechtliche Vorschriften erlangt wurden, ist insbesondere anhand der Gefahr zu beurteilen, die mit der Zulässigkeit solcher Informationen und Beweise für die Wahrung des Grundsatzes des kontradiktorischen Verfahrens und damit für das Recht auf ein faires Verfahren verbunden ist. Kommt ein Gericht zu dem Ergebnis, dass eine Partei nicht in der Lage ist, sachgerecht zu einem Beweismittel Stellung zu nehmen, das einem Bereich entstammt, in dem das Gericht nicht über Sachkenntnis verfügt, und das geeignet ist, die Würdigung der Tatsachen maßgeblich zu beeinflussen, muss es eine Verletzung des Rechts auf ein faires Verfahren feststellen und dieses Beweismittel ausschließen, um eine solche Rechtsverletzung zu verhindern. Der Effektivitätsgrundsatz verpflichtet ein nationales Strafgericht somit dazu, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten oder durch einen unionsrechtswidrigen Zugang der zuständigen Behörde zu den fraglichen Daten erlangt wurden, auszuschließen, sofern diese Personen nicht in der Lage sind, sachgerecht zu den Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen (vgl. in diesem Sinne 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. 226 und 227).

45 Nach alledem ist auf die erste und die zweite Frage 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 Regelung entgegensteht, die es Behörden zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten ermöglicht, Zugang zu einem Satz von Verkehrs- oder Standortdaten zu erlangen, die geeignet sind, Informationen über die von einem Nutzer eines elektronischen Kommunikationsmittels getätigten Kommunikationen oder über den Standort der von ihm verwendeten Endgeräte zu liefern und genaue Schlüsse auf sein Privatleben zuzulassen, ohne dass sich dieser Zugang auf Verfahren zur Bekämpfung schwerer Kriminalität oder zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit beschränken würde; dies gilt unabhängig davon, für welchen Zeitraum der Zugang zu den betreffenden Daten begehrt wird und welche Menge oder Art von Daten für einen solchen Zeitraum verfügbar ist.

Zur dritten Frage

46 Mit der dritten Vorlagefrage möchte das vorlegende Gericht 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 einer nationalen Regelung entgegensteht, wonach die Staatsanwaltschaft, deren Aufgabe darin besteht, das strafrechtliche Ermittlungsverfahren zu leiten und gegebenenfalls in einem späteren Verfahren die öffentliche Klage zu vertreten, dafür zuständig ist, einer Behörde für strafrechtliche Ermittlungen Zugang zu Verkehrs- und Standortdaten zu gewähren.

47 Das vorlegende Gericht führt hierzu aus, die estnische Staatsanwaltschaft sei zwar nach nationalem Recht verpflichtet, unabhängig zu handeln, sei nur dem Gesetz unterworfen und müsse im Ermittlungsverfahren alle belastenden und entlastenden Gesichtspunkte prüfen. Gleichwohl bestehe das Ziel dieses Verfahrens darin, Beweise zu erheben sowie die übrigen Voraussetzungen für ein gerichtliches Verfahren zu erfüllen. Dieselbe Behörde vertrete vor dem Gericht die öffentliche Klage und sei damit auch am Verfahren beteiligt. Ferner geht aus den dem Gerichtshof vorliegenden Akten hervor, dass die estnische Staatsanwaltschaft hierarchisch aufgebaut ist und dass Anträge auf Zugang zu Verkehrs- und Standortdaten keinem besonderen Formerfordernis unterliegen und vom Staatsanwalt selbst gestellt werden können; dies ist auch von der estnischen Regierung und der Prokuratuur in der mündlichen Verhandlung bestätigt worden. Schließlich handelt es sich bei den Personen, deren Daten zugänglich gemacht werden können, nicht nur um diejenigen, die im Verdacht der Beteiligung an einer Straftat stehen.

48 Wie der Gerichtshof bereits entschieden hat, sind zwar die Voraussetzungen, unter denen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den Daten gewähren müssen, über die sie verfügen, im nationalen Recht festzulegen. Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss eine solche Regelung jedoch klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, damit die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken ermöglichen. Die Regelung muss nach innerstaatlichem Recht bindend sein und Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, um zu gewährleisten, dass sich der Eingriff auf das absolut Notwendige beschränkt (vgl. in diesem Sinne Urteile vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 117 und 118, vom 6. Oktober 2020, Privacy International, C-623/17, EU:C:2020:790, Rn. 68, und 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. 132 und die dort angeführte Rechtsprechung).

49 Insbesondere darf sich eine nationale Regelung über den Zugang der zuständigen Behörden zu gespeicherten Verkehrs- und Standortdaten, die aufgrund von Art. 15 Abs. 1 der Richtlinie 2002/58 erlassen wurde, nicht darauf beschränken, dass der behördliche Zugang zu den Daten dem mit der Regelung verfolgten Zweck zu entsprechen hat, sondern muss auch die materiellen und prozeduralen Voraussetzungen für die Verwendung der Daten vorsehen (Urteile vom 6. Oktober 2020, Privacy International, C-623/17, EU:C:2020:790, Rn. 77, und 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. 176 und die dort angeführte Rechtsprechung).

50 Infolgedessen, und weil ein allgemeiner Zugang zu allen gespeicherten Daten unabhängig davon, ob irgendein – zumindest mittelbarer – Zusammenhang mit dem verfolgten Ziel besteht, nicht als auf das absolut Notwendige beschränkt angesehen werden kann, muss sich die betreffende nationale Regelung 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. Insoweit darf im Zusammenhang mit dem Ziel, die Kriminalität zu bekämpfen, ein solcher Zugang grundsätzlich nur zu den Daten von Personen gewährt werden, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche

Straftat verwickelt zu sein. Allerdings könnte in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, auch Zugang zu Daten anderer Personen gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung derartiger Aktivitäten leisten könnten (vgl. in diesem Sinne Urteile vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 119, und 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. 188).

51 Um in der Praxis die vollständige Einhaltung dieser Voraussetzungen zu gewährleisten, ist es unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und dass dessen oder deren Entscheidung auf einen mit Gründen versehenen, von den zuständigen nationalen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellten Antrag ergeht. In hinreichend begründeten Eilfällen muss die Kontrolle kurzfristig erfolgen (vgl. in diesem Sinne 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. 189 und die dort angeführte Rechtsprechung).

52 Diese vorherige Kontrolle setzt, wie der Generalanwalt im Wesentlichen in Nr. 105 seiner Schlussanträge ausgeführt hat, u. a. voraus, dass das mit ihr betraute Gericht oder die mit ihr betraute Stelle über alle Befugnisse verfügt und alle Garantien aufweist, die erforderlich sind, um zu gewährleisten, dass die verschiedenen einander gegenüberstehenden Interessen und Rechte in Einklang gebracht werden. Im Fall strafrechtlicher Ermittlungen verlangt eine solche Kontrolle, dass dieses Gericht oder diese Stelle in der Lage ist, für einen gerechten Ausgleich zwischen den Interessen, die sich aus den Erfordernissen der Ermittlungen im Rahmen der Kriminalitätsbekämpfung ergeben, und den Grundrechten auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten der Personen, auf deren Daten zugegriffen wird, zu sorgen.

53 Wird die Kontrolle nicht von einem Gericht, sondern von einer unabhängigen Verwaltungsstelle wahrgenommen, muss diese über eine Stellung verfügen, die es ihr erlaubt, bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorzugehen, ohne jede Einflussnahme von außen (vgl. in diesem Sinne Urteil vom 9. März 2010, Kommission/Deutschland, C-518/07, EU:C:2010:125, Rn. 25, sowie Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 229 und 230].

54 Aus den vorstehenden Erwägungen folgt, dass das in Rn. 51 des vorliegenden Urteils angeführte Erfordernis, wonach die mit der Wahrnehmung der vorherigen Kontrolle betraute Behörde unabhängig sein muss, es gebietet, dass es sich bei ihr um eine andere als die den Zugang zu den Daten begehrende Stelle handelt, damit Erstere in der Lage ist, diese Kontrolle objektiv und unparteiisch, ohne jede Einflussnahme von außen, auszuüben. Im strafrechtlichen Bereich impliziert das Erfordernis der Unabhängigkeit, wie der Generalanwalt im Wesentlichen in Nr. 126 seiner Schlussanträge ausgeführt hat, insbesondere, dass die mit der vorherigen Kontrolle betraute Behörde zum einen nicht an der Durchführung des fraglichen Ermittlungsverfahrens beteiligt ist und zum anderen eine Position der Neutralität gegenüber den Beteiligten am Strafverfahren hat.

55 Bei einer Staatsanwaltschaft, die das Ermittlungsverfahren leitet und gegebenenfalls die öffentliche Klage vertritt, ist dies nicht der Fall. Die Aufgabe der Staatsanwaltschaft besteht nämlich nicht darin, über eine Rechtssache in voller Unabhängigkeit zu entscheiden, sondern darin, sie gegebenenfalls als Beteiligte am Strafprozess dem zuständigen Gericht zu unterbreiten.

56 Der Umstand, dass die Staatsanwaltschaft gemäß den Regeln über ihre Zuständigkeiten und ihren Status verpflichtet ist, die belastenden und entlastenden Gesichtspunkte zu prüfen sowie die Rechtmäßigkeit des Ermittlungsverfahrens zu gewährleisten, wobei sie nur an das Gesetz und die

eigene Überzeugung gebunden ist, reicht nicht aus, um ihr die Stellung eines Dritten im Verhältnis zu den einander gegenüberstehenden Interessen in dem in Rn. 52 des vorliegenden Urteils beschriebenen Sinn zu verleihen.

57 Folglich ist die Staatsanwaltschaft nicht in der Lage, die in Rn. 51 des vorliegenden Urteils angesprochene vorherige Kontrolle wahrzunehmen.

58 Zu der vom vorlegenden Gericht darüber hinaus aufgeworfenen Frage, ob die fehlende Kontrolle seitens einer unabhängigen Behörde durch eine spätere gerichtliche Kontrolle der Rechtmäßigkeit des Zugangs einer nationalen Behörde zu Verkehrs- und Standortdaten ausgeglichen werden kann, ist festzustellen, dass die unabhängige Kontrolle nach der in Rn. 51 des vorliegenden Urteils angeführten Rechtsprechung vor jedem Zugang stattfinden muss, abgesehen von hinreichend begründeten Eilfällen, in denen sie kurzfristig erfolgen muss. Wie der Generalanwalt in Nr. 128 seiner Schlussanträge ausgeführt hat, würde eine solche spätere Kontrolle es nicht ermöglichen, das Ziel der vorherigen Kontrolle zu erreichen, das darin besteht, zu verhindern, dass ein über das absolut Notwendige hinausgehender Zugang zu den fraglichen Daten genehmigt wird.

59 Unter diesen Umständen ist auf die dritte 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 Regelung entgegensteht, wonach die Staatsanwaltschaft, deren Aufgabe darin besteht, das strafrechtliche Ermittlungsverfahren zu leiten und gegebenenfalls in einem späteren Verfahren die öffentliche Klage zu vertreten, dafür zuständig ist, einer Behörde für strafrechtliche Ermittlungen Zugang zu Verkehrs- und Standortdaten zu gewähren.

Kosten

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

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

1. **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 Regelung entgegensteht, die es Behörden zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten ermöglicht, Zugang zu einem Satz von Verkehrs- oder Standortdaten zu erlangen, die geeignet sind, Informationen über die von einem Nutzer eines elektronischen Kommunikationsmittels getätigten Kommunikationen oder über den Standort der von ihm verwendeten Endgeräte zu liefern und genaue Schlüsse auf sein Privatleben zuzulassen, ohne dass sich dieser Zugang auf Verfahren zur Bekämpfung schwerer Kriminalität oder zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit beschränken würde; dies gilt unabhängig davon, für welchen Zeitraum der Zugang zu den betreffenden Daten begehrt wird und welche Menge oder Art von Daten für einen solchen Zeitraum verfügbar ist.**

2. **Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung entgegensteht, wonach die Staatsanwaltschaft, deren Aufgabe darin besteht, das strafrechtliche Ermittlungsverfahren zu**

leiten und gegebenenfalls in einem späteren Verfahren die öffentliche Klage zu vertreten, dafür zuständig ist, einer Behörde für strafrechtliche Ermittlungen Zugang zu Verkehrs- und Standortdaten zu gewähren.

Unterschriften