ENTSCHEIDUNGEN

Vorratsdatenspeicherung 3.0 – Allgemeine und unterschiedslose Vorratsdatenspeicherung von Verkehrs- und Standortdaten ohne Anlass unzulässig

EuGH, Urt. v. 6.10.2020 – C-511/18, C-512/18 und C-520/18

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 Rechtsvorschriften entgegensteht, die zu den in Art. 15 Abs. 1 genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Dagegen steht Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte Rechtsvorschriften nicht entgegen, die

- **es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht;**

- **zum Schutz der nationalen Sicherheit, 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;**

- **zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;**

- **zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;**

- **es zur Bekämpfung schwerer Kriminalität und, *a fortiori*, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.**

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung 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.

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 nicht entgegensteht, mit der den Betreibern elektronischer Kommunikationsdienste auferlegt wird, zum einen eine automatisierte Analyse sowie eine Erhebung in Echtzeit insbesondere von Verkehrs- und Standortdaten und zum anderen eine Erhebung in Echtzeit der technischen Daten zum Standort der verwendeten Endgeräte vorzunehmen, sofern

- **der Rückgriff auf die automatisierte Analyse auf Situationen beschränkt ist, in denen sich ein Mit-**

gliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, und Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer die fragliche Maßnahme rechtfertigenden Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und

- **der Rückgriff auf die Erhebung von Verkehrs- und Standortdaten in Echtzeit auf Personen beschränkt ist, bei denen ein triftiger Grund für den Verdacht besteht, dass sie auf irgendeine Weise in terroristische Aktivitäten verwickelt sind, und einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegt, deren Entscheidung bindend ist, wobei dieses Gericht oder diese Stelle sich vergewissern muss, dass eine solche Erhebung in Echtzeit nur in den Grenzen des absolut Notwendigen gestattet wird. In hinreichend begründeten Eilfällen muss die Kontrolle kurzfristig erfolgen.**

3. Die Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr") ist dahin auszulegen, dass sie im Bereich des Schutzes der Vertraulichkeit der Kommunikation sowie des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten im Rahmen der Dienste der Informationsgesellschaft nicht anwendbar ist; dieser Schutz ist entweder durch die Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung oder durch 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 geregelt. Art. 23 Abs. 1 der Verordnung 2016/679 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, mit der den Anbietern eines öffentlichen Online- Zugangs zu Kommunikationsdiensten und den Betreibern von Hosting-Diensten eine allgemeine und unterschiedslose Vorratsspeicherung insbesondere von personenbezogenen Daten im Zusammenhang mit diesen Diensten auferlegt wird.

4. Ein nationales Gericht darf eine Bestimmung seines nationalen Rechts nicht anwenden, die es ermächtigt, die ihm nach nationalem Recht obliegende Feststellung, dass nationale Rechtsvorschriften, mit denen den Betreibern elektronischer Kommunikationsdienste u.a. zur Verfolgung der Ziele des Schutzes der nationalen Sicherheit und der Bekämpfung der Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird, wegen ihrer Unvereinbarkeit mit Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte rechtswidrig sind, in ihren zeitlichen Wirkungen zu beschränken. Art. 15 Abs. 1 der Richtlinie verpflichtet bei einer Auslegung im Licht des Effektivitätsgrundsatzes ein nationales Strafgericht dazu, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen 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.

[…]

Urteil

1 Die Vorabentscheidungsersuchen betreffen die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 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 25.11.2009 (ABl. 2009, L 337, S. 11) geänderten Fassung (im Folgenden: Richtlinie 2002/58) sowie der Art. 12 bis 15 der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr") (ABl. 2000, L 178, S. 1) im Licht der Art. 4, 6 bis 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) und von Art. 4 Abs. 2 EUV.

[…]

Zu den Vorlagefragen

Zur ersten Frage in den Rechtssachen C−511/18 und C−512/18 sowie zur ersten und zur zweiten Frage in der Rechtssache C−520/18

81 Mit der ersten Frage in den Rechtssachen C−511/18 und C−512/18 sowie der ersten und der zweiten Frage in der Rechtssache C−520/18, die zusammen zu prüfen sind, möchten die vorlegenden Gerichte wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die die Betreiber elektronischer Kommunikationsdienste zu den in Art. 15 Abs. 1 genannten Zwecken zur allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten verpflichtet.

Vorbemerkungen

82 Aus den Akten, die dem *Gerichtshof* vorliegen, geht hervor, dass sich die in den Ausgangsverfahren in Rede stehenden Regelungen auf alle elektronischen Kommunikationsmittel und alle ihre Nutzer erstrecken, ohne dass es insoweit eine Differenzierung oder Ausnahme gibt. Außerdem handelt es sich bei den Daten, die nach diesen Regelungen von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert werden müssen, insbesondere um solche, die erforderlich sind, um die Quelle und den Adressaten einer Kommunikation aufzuspüren, Datum, Uhrzeit, Dauer und Art der Kommunikation zu ermitteln, das verwendete Kommunikationsmaterial zu identifizieren sowie den Standort der Endgeräte und der Kommunikationen zu bestimmen. Zu diesen Daten gehören u. a. Name und Adresse des Nutzers, die Telefonnummern des Anrufers und des Angerufenen sowie die IP-Adresse für die Internetdienste. Auf den Inhalt der betreffenden Kommunikationen erstrecken sie sich dagegen nicht.

83 Den Daten, die nach den in den Ausgangsverfahren in Rede stehenden nationalen Regelungen ein Jahr lang gespeichert werden müssen, lässt sich somit u. a. entnehmen, mit welcher Person der Nutzer eines elektronischen Kommunikationsmittels kommuniziert hat und mit welchem Mittel dies stattfand, das Datum, die Uhrzeit und die Dauer der Kommunikationen und der Internetverbindungen sowie der Ort, von dem aus sie stattfanden, ohne dass zwangsläufig eine Kommunikation weitergeleitet wurde. Außerdem bieten sie die Möglichkeit, die Häufigkeit der Kommunikationen des Nutzers mit bestimmten Personen während eines konkreten Zeitraums zu ermitteln. Schließlich ermöglicht die in den Rechtssachen C-511/18 und C-512/18 in Rede stehende nationale Regelung, da sie sich auch auf Daten in Bezug auf die Weiterleitung der elektronischen Kommunikationen durch die Netze erstreckt, offenbar überdies die Identifizierung der Art online konsultierter Informationen.

84 Zu den verfolgten Zielen ist festzustellen, dass zu den Zielen, die mit den Regelungen, um die es in den Rechtssachen C-511/18 und C-512/18 geht, verfolgt werden, u. a. die Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen, die nationale Unabhängigkeit, die Integrität des Hoheitsgebiets und die nationale Verteidigung, die wichtigen Interessen der Außenpolitik, die Erfüllung der europäischen und internationalen Verpflichtungen Frankreichs, die wichtigen wirtschaftlichen, industriellen und wissenschaftlichen Interessen Frankreichs sowie die Verhütung des Terrorismus, von Beeinträchtigungen des republikanischen Charakters der Institutionen und von kollektiver Gewalt, die geeignet ist, den öffentlichen Frieden schwer zu beeinträchtigen, erfassen. Die Regelung, um die es in der Rechtssache C-520/18 geht, dient u. a. zur Ermittlung, Feststellung und Verfolgung von Straftaten sowie zum Schutz der nationalen Sicherheit, der Landesverteidigung und der öffentlichen Sicherheit.

85 Die vorlegenden Gerichte werfen insbesondere die Frage nach den etwaigen Auswirkungen des in Art. 6 der Charta verankerten Rechts auf Sicherheit auf die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 auf. Ferner möchten sie wissen, ob der mit der Vorratsspeicherung von Daten, die in den Regelungen, um die es in den Ausgangsverfahren geht, vorgesehen ist, verbundene Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte angesichts der bestehenden Vorschriften, die den Zugang nationaler Behörden zu den gespeicherten Daten beschränken, als gerechtfertigt angesehen werden kann. Außerdem muss diese Frage nach Ansicht des Conseil d'État (Staatsrat), da sie sich in einem durch ernste und anhaltende Bedrohungen der nationalen Sicherheit gekennzeichneten Kontext stellt, auch anhand von Art. 4 Abs. 2 EUV beurteilt werden. Der *Verfassungsgerichtshof* hebt hervor, dass mit der nationalen Regelung, um die es in der Rechtssache C-520/18 gehe, auch positive Verpflichtungen umgesetzt würden, die sich aus den Art. 4 und 7 der Charta ergäben und die darin bestünden, einen gesetzlichen Rahmen vorzusehen, der eine wirksame Ahndung des sexuellen Missbrauchs von Minderjährigen ermögliche.

[…]

Zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58

105 Einleitend ist darauf hinzuweisen, dass nach ständiger Rechtsprechung bei der Auslegung einer unionsrechtlichen Vorschrift nicht nur ihr Wortlaut zu berücksichtigen ist, sondern auch ihr Kontext und die Ziele, die mit der Regelung, zu der sie gehört, verfolgt werden, und insbesondere deren Entstehungsgeschichte (vgl. in diesem Sinne Urt. v. 17.4.2018, *Egenberger*, C-414/16, EU:C:2018:257, Rn. 44).

106 Die Richtlinie 2002/58 soll, wie sich u. a. aus ihren Erwägungsgründen 6 und 7 ergibt, die Nutzer elektronischer Kommunikationsdienste vor den Risiken für ihre personenbezogenen Daten und ihre Privatsphäre schützen, die sich aus den neuen Technologien und vor allem den zunehmenden Fähigkeiten zur automatisierten Speicherung und Verarbeitung von Daten ergeben. Insbesondere soll mit der Richtlinie nach ihrem zweiten Erwägungsgrund gewährleistet werden, dass die in den Art. 7 und 8 der Charta niedergelegten Rechte uneingeschränkt geachtet werden. Insoweit ergibt sich aus der Begründung des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM[2000] 385 endg.), aus dem die Richtlinie 2002/58 hervorgegangen ist, dass der Unionsgesetzgeber sicherstellen wollte, „dass für alle elektronischen Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie weiterhin ein hochgradiger Schutz personenbezogener Daten und der Privatsphäre gewährleistet bleibt".

107 Zu diesem Zweck wird in Art. 5 Abs. 1 der Richtlinie 2002/58 der Grundsatz der Vertraulichkeit sowohl elektronischer Nachrichten als auch der damit verbundenen Verkehrsdaten aufgestellt, der u.a. das grundsätzliche Verbot für jede andere Person als die Nutzer, ohne deren Einwil-

ligung solche Nachrichten und Daten auf Vorrat zu speichern, impliziert.

108 Insbesondere ergibt sich hinsichtlich der Verarbeitung und Speicherung von Verkehrsdaten durch die Betreiber elektronischer Kommunikationsdienste aus Art. 6 sowie den Erwägungsgründen 22 und 26 der Richtlinie 2002/58, dass eine solche Verarbeitung nur zur Gebührenabrechnung für die Dienste, zu deren Vermarktung und zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu erforderlichen Zeitraums zulässig ist. Danach sind die verarbeiteten und gespeicherten Daten zu löschen oder zu anonymisieren. Andere Standortdaten als Verkehrsdaten dürfen nach Art. 9 Abs. 1 der Richtlinie nur unter bestimmten Voraussetzungen und nur dann verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben (Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 86 und die dort angeführte Rechtsprechung).

109 Durch den Erlass dieser Richtlinie hat der Unionsgesetzgeber somit die in den Art. 7 und 8 der Charta verankerten Rechte konkretisiert, so dass die Nutzer elektronischer Kommunikationsmittel grundsätzlich erwarten dürfen, dass ihre Nachrichten und die damit verbundenen Verkehrsdaten anonym bleiben und nicht gespeichert werden dürfen, es sei denn, sie haben darin eingewilligt.

110 Art. 15 Abs. 1 der Richtlinie 2002/58 gestattet es den Mitgliedstaaten jedoch, 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.

111 Die Befugnis, von den Rechten und Pflichten, wie sie die Art. 5, 6 und 9 der Richtlinie 2002/58 vorsehen, abzuweichen, kann es aber nicht rechtfertigen, dass die Ausnahme von dieser grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Daten und insbesondere von dem in Art. 5 der Richtlinie ausdrücklich vorgesehenen Verbot, solche Daten zu speichern, zur Regel wird (vgl. in diesem Sinne Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 89 und 104).

112 Hinsichtlich der Zwecke, 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 Art. 15 Abs. 1 S. 1 der Richtlinie genannten Zwecke abschließend ist, so dass eine aufgrund dieser Bestimmung erlassene Rechtsvorschrift tatsächlich strikt einem von ihnen dienen muss (vgl. in diesem Sinne Urt. v. 2.10.2018, Ministerio Fiscal, C−207/16, EU:C:2018:788, Rn. 52 und die dort angeführte Rechtsprechung).

113 Außerdem geht aus Art. 15 Abs. 1 S. 3 der Richtlinie 2002/58 hervor, dass die Mitgliedstaaten Rechtsvorschriften, die die Tragweite der Rechte und Pflichten gemäß den Art. 5, 6 und 9 dieser Richtlinie beschränken sollen, nur unter Beachtung der allgemeinen Grundsätze des Unionsrechts, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und der durch die Charta garantierten Grundrechte erlassen dürfen. Hierzu hat der *Gerichtshof* bereits entschieden, dass die den Betreibern elektronischer Kommunikationsdienste durch eine nationale Regelung auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, Fragen aufwirft, die nicht nur die Einhaltung der die Achtung des Privatlebens und den Schutz personenbezogener Daten garantierenden Art. 7 und 8 der Charta betreffen, sondern auch der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung (vgl. in diesem Sinne Urt. v. 8.4.2014, Digital Rights, C−293/12 und C−594/12, EU:C:2014:238, Rn. 25 und 70, sowie v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 91 und 92 sowie die dort angeführte Rechtsprechung).

114 Bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 muss somit die Bedeutung sowohl des in Art. 7 der Charta gewährleisteten Rechts auf Achtung des Privatlebens als auch des in Art. 8 der Charta gewährleisteten Rechts auf den Schutz personenbezogener Daten, wie sie sich aus der Rechtsprechung des *Gerichtshofs* ergibt, berücksichtigt werden sowie das in Art. 11 der Charta gewährleistete Recht auf freie Meinungsäußerung, das eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Union nach Art. 2 EUV gründet (vgl. in diesem Sinne Urt. v. 6.3.2001, Connolly/Kommission, C−274/99 P, EU:C:2001:127, Rn. 39, und v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 93 und die dort angeführte Rechtsprechung).

115 Insoweit ist darauf hinzuweisen, dass die Speicherung der Verkehrs- und Standortdaten als solche zum einen eine Abweichung von dem nach Art. 5 Abs. 1 der Richtlinie 2002/58 für alle anderen Personen als die Nutzer geltenden Verbot der Speicherung dieser Daten darstellt und zum anderen einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, die in den Art. 7 und 8 der Charta verankert sind; dabei spielt es keine Rolle, ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben und ob die Betroffenen durch diesen Eingriff Nachteile erlitten haben (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] v. 26.7.2017, EU:C:2017:592, Rn. 124 und 126 sowie die dort angeführte Rechtsprechung; vgl. entsprechend, in Bezug auf Art. 8 der EMRK, *EGMR*, Urt. v. 30.1.2020, Breyer gegen

Deutschland, CE:ECHR:2020:0130JUD005000112, § 81).

116 Irrelevant ist auch, ob die gespeicherten Daten in der Folge verwendet werden (vgl. entsprechend, in Bezug auf Art. 8 der EMRK, *EGMR*, Urt. v. 16.2.2000, Amann gegen Schweiz, CE:ECHR:2000:0216JUD002779895, § 69, sowie Urt. v. 13.2.2020, Trjakovski und Chipovski gegen Nordmazedonien, CE:ECHR:2020:0213JUD005 320513, § 51), da der Zugriff auf solche Daten, unabhängig von ihrer späteren Verwendung, einen gesonderten Eingriff in die in der vorstehenden Randnummer genannten Grundrechte darstellt (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26.7.2017, EU:C:2017:592, Rn. 124 und 126).

117 Dieser Schluss erscheint umso gerechtfertigter, als die Verkehrs- und Standortdaten Informationen über eine Vielzahl von Aspekten des Privatlebens der Betroffenen enthalten können, einschließlich sensibler Informationen wie sexuelle Orientierung, politische Meinungen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen sowie den Gesundheitszustand, wobei solche Daten im Übrigen im Unionsrecht besonderen Schutz genießen. Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, gezogen werden, 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. Diese Daten ermöglichen insbesondere die Erstellung eines Profils der Betroffenen, das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible Information darstellt wie der Inhalt der Kommunikationen selbst (vgl. in diesem Sinne Urt. v. 8.4.2014, Digital Rights, C−293/12 und C−594/12, EU:C:2014:238, Rn. 27, und v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 99).

118 Daher kann die Vorratsspeicherung von Verkehrs- und Standortdaten zu polizeilichen Zwecken zum einen für sich genommen das in Art. 7 der Charta verankerte Recht auf Achtung der Kommunikation beeinträchtigen und die Nutzer elektronischer Kommunikationsmittel von der Ausübung ihrer durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung abhalten (vgl. in diesem Sinne Urt. v. 8.4.2014, Digital Rights, C−293/12 und C−594/12, EU:C:2014:238, Rn. 28, und v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 101). Solche abschreckenden Wirkungen können in besonderem Maß Personen treffen, deren Kommunikationen nach den nationalen Vorschriften dem Berufsgeheimnis unterliegen, sowie Whistleblower, deren Aktivitäten durch die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (ABl. 2019, L 305, S. 17), geschützt werden. Außerdem sind diese Wirkungen umso stärker, je größer die Menge und die Vielfalt der auf Vorrat gespeicherten Daten sind.

119 Zum anderen birgt die bloße Vorratsspeicherung durch die Betreiber elektronischer Kommunikationsdienste angesichts der großen Menge von Verkehrs- und Standortdaten, die durch eine Maßnahme allgemeiner und unterschiedsloser Vorratsspeicherung kontinuierlich gespeichert werden können, sowie des sensiblen Charakters der Informationen, die diese Daten liefern können, Gefahren des Missbrauchs und des rechtswidrigen Zugangs.

120 In Art. 15 Abs. 1 der Richtlinie 2002/58, der es den Mitgliedstaaten gestattet, die in Rn. 110 des vorliegenden Urteils angesprochenen Ausnahmen vorzusehen, kommt allerdings zum Ausdruck, dass die in den Art. 7, 8 und 11 der Charta verankerten Rechte keine uneingeschränkte Geltung beanspruchen können, sondern im Hinblick auf ihre gesellschaftliche Funktion gesehen werden müssen (vgl. in diesem Sinne Urt. v. 16.7.2020, Facebook Ireland und Schrems, C−311/18, EU:C:2020:559, Rn. 172 und die dort angeführte Rechtsprechung).

121 Nach Art. 52 Abs. 1 der Charta sind nämlich Einschränkungen der Ausübung dieser Rechte zulässig, sofern sie gesetzlich vorgesehen sind und den Wesensgehalt dieser Rechte achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit müssen sie erforderlich sein und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

122 Bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Charta muss somit auch berücksichtigt werden, welche Bedeutung den in den Art. 3, 4, 6 und 7 der Charta verankerten Rechten und den Zielen des Schutzes der nationalen Sicherheit und der Bekämpfung schwerer Kriminalität als Beitrag zum Schutz der Rechte und Freiheiten anderer zukommt.

123 Insoweit ist in Art. 6 der Charta, auf den der Conseil d'État (Staatsrat) und der *Verfassungsgerichtshof* Bezug nehmen, das Recht jedes Menschen nicht nur auf Freiheit, sondern auch auf Sicherheit verankert, und er garantiert Rechte, die den durch Art. 5 der EMRK garantierten Rechten entsprechen (vgl. in diesem Sinne Urt. v. 15.2.2016, N., C−601/15 PPU, EU:C:2016:84, Rn. 47, Urt. v. 28.7 . 2016, JZ, C−294/16 PPU, EU:C:2016:610, Rn. 48, und v. 19.9.2019, Rayonna prokuratura Lom, C−467/18, EU:C:2019:765, Rn. 42 und die dort angeführte Rechtsprechung).

124 Ferner ist darauf hinzuweisen, dass mit Art. 52 Abs. 3 der Charta die notwendige Kohärenz zwischen den in der Charta enthaltenen Rechten und den entsprechenden durch die EMRK garantierten Rechten gewährleistet werden soll, ohne dass dadurch die Eigenständigkeit des Unionsrechts und des *Gerichtshofs der Europäischen Union* berührt wird. Bei der Auslegung der Charta sind somit die entsprechenden Rechte der EMRK als Mindestschutzstandard zu berücksichtigen (vgl. in diesem Sinne Urt. v. 12.2.2019, TC, C−492/18 PPU, EU:C:2019:108, Rn. 57, und Urt. v. 21.5.2019, Kommission/Ungarn [Nießbrauchsrechte an landwirtschaftlichen Flächen], C−235/17, EU:C:2019:432, Rn. 72 und die dort angeführte Rechtsprechung).

125 Art. 5 der EMRK, in dem das Recht auf Freiheit und das Recht auf Sicherheit verankert sind, soll nach der Rechtsprechung des *Europäischen Gerichtshofs für Menschenrechte* den Einzelnen vor jedem willkürlichen oder ungerechtfertigten Freiheitsentzug schützen (vgl. in diesem Sinne *EGMR*, Urt. v. 18.3.2008, Ladent gegen Polen, CE:ECHR:2008:0318JUD001103603, §§ 45 und 46, Urt. v. 29.3.2010, Medvedyev und andere gegen Frankreich, CE:ECHR:2010:0329JUD000339403, §§ 76 und 77, sowie Urt. v. 13.12.2012, El−Masri gegen „The former Yugoslav Republic of Macedonia", CE:ECHR:2012:1213JUD003963009, § 239). Da diese Bestimmung einenFreiheitsentzug durch eine staatliche Stelle betrifft, kann Art. 6 der Charta jedoch nicht dahin ausgelegt werden, dass er die staatlichen Stellen verpflichtet, spezifische Maßnahmen zur Ahndung bestimmter Straftaten zu erlassen.

126 In Bezug insbesondere auf die vom *Verfassungsgerichtshof* angesprochene wirksame Bekämpfung von Straftaten, deren Opfer u.a. Minderjährige und andere schutzbedürftige Personen sind, ist hingegen hervorzuheben, dass sich aus Art. 7 der Charta positive Verpflichtungen der Behörden im Hinblick auf den Erlass rechtlicher Maßnahmen zum Schutz des Privat- und Familienlebens ergeben können (vgl. in diesem Sinne Urt. v. 18.6.2020, Kommission/Ungarn [Transparenz von Vereinigungen], C−78/18, EU:C:2020:476, Rn. 123 und die dort angeführte Rechtsprechung des *Europäischen Gerichtshofs für Menschenrechte*). Solche Verpflichtungen können sich aus Art. 7 auch in Bezug auf den Schutz der Wohnung und der Kommunikation sowie aus den Art. 3 und 4 hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit der Menschen sowie des Verbots der Folter und unmenschlicher oder erniedrigender Behandlung ergeben.

127 Angesichts dieser verschiedenen positiven Verpflichtungen müssen die verschiedenen betroffenen Interessen und Rechte miteinander in Einklang gebracht werden.

128 Der *EGMR* hat nämlich entschieden, dass die den Art. 3 und 8 der EMRK zu entnehmenden positiven Verpflichtungen, denen die Garantien in den Art. 4 und 7der Charta entsprechen, u. a. bedeuten, dass materielle und prozedurale Vorschriften zu erlassen sowie praktische Maßnahmen zu treffen sind, die eine wirksame Bekämpfung von Straftaten gegen Personen mittels effektiver Ermittlungen und Verfolgung gestatten. Diese Verpflichtung ist umso wichtiger, wenn das körperliche und geistige Wohlergehen eines Kindes bedroht ist. Die von den zuständigen Behörden zu treffenden Maßnahmen müssen aber den Rechtsschutzmöglichkeiten und übrigen Garantien, die geeignet sind, den Umfang der strafrechtlichen Ermittlungsbefugnisse zu begrenzen, sowie den sonstigen Freiheiten und Rechten umfassend Rechnung tragen. Insbesondere ist ein rechtlicher Rahmen zu schaffen, der es erlaubt, die verschiedenen zu schützenden Interessen und Rechte miteinander in Einklang zu bringen (*EGMR*, Urt. v. 28.10.1998, Osman gegen Vereinigtes Königreich, CE:ECHR:1998:1028JUD002345294, §§ 115 und 116, Urt. v. 4.3.2004, M.C. gegen Bulgarien, CE:ECHR:2003:1204JUD003927298, § 151, Urt. v. 24.6.2004, Von Hannover gegen Deutschland, CE:ECHR:2004:0624JUD005932000, §§ 57 und 58, sowie 2. Dezember 2008, K.U. gegen Finnland, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 und 49).

129 In Bezug auf die Beachtung des Grundsatzes der Verhältnismäßigkeit sieht Art. 15 Abs. 1 S. 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten eine Vorschrift erlassen können, die vom Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweicht, sofern dies in Anbetracht der dort genannten Zwecke „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig" ist. Im elften Erwägungsgrund der Richtlinie wird klargestellt, dass eine derartige Maßnahme in einem „strikt" angemessenen Verhältnis zum intendierten Zweck stehen muss.

130 Insoweit ist darauf hinzuweisen, dass der Schutz des Grundrechts auf Achtung des Privatlebens nach ständiger Rechtsprechung des *Gerichtshofs* verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken. Außerdem kann eine dem Gemeinwohl dienende Zielsetzung nicht verfolgt werden, ohne den Umstand zu berücksichtigen, dass sie mit den von der Maßnahme betroffenen Grundrechten in Einklang gebracht werden muss, indem eine ausgewogene Gewichtung der dem Gemeinwohl dienenden Zielsetzung und der fraglichen Rechte vorgenommen wird (vgl. in diesem Sinne Urt. v. 16.12.2008, Satakunnan Markkinapörssi und Satamedia, C−73/07, EU:C:2008:727, Rn. 56, v. 9.11.2010, Volker und Markus Schecke und Eifert, C−92/09 und C−93/09, EU:C:2010:662, Rn. 76, 77 und 86, sowie Urt. v. 8.4.2014, Digital Rights, C−293/12 und C−594/12, EU:C:2014:238, Rn. 52; Gutachten 1/15 [PNR-Abkommen EU–Kanada] v. 26.7.2017, EU:C:2017:592, Rn. 140).

131 Insbesondere geht aus der Rechtsprechung des *Gerichtshofs* hervor, 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 verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zur Schwere des Eingriffs steht (vgl. in diesem Sinne Urt. v. 2.10.2018, Ministerio Fiscal, C−207/16, EU:C:2018:788, Rn. 55 und die dort angeführte Rechtsprechung).

132 Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss eine Regelung klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz dieser Daten vor Missbrauchsrisiken ermöglichen. Die Regelung muss nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten

vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisiert verarbeitet werden, vor allem wenn eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht. Diese Erwägungen gelten in besonderem Maß, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht (vgl. in diesem Sinne Urt. v. 8.4.2014, Digital Rights, C−293/12 und C−594/12, EU:C:2014:238, Rn. 54 und 55, sowie Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 117; Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26.7.2017, EU:C:2017:592, Rn. 141).

133 Eine Regelung, die eine Vorratsspeicherung personenbezogener Daten vorsieht, muss daher stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26.7.2017, EU:C:2017:592, Rn. 191 und die dort angeführte Rechtsprechung, sowie Urt. v. 3.10.2019, A u. a., C−70/18, EU:C:2019:823, Rn. 63).

Zu den Rechtsvorschriften, die zum Schutz der nationalen Sicherheit eine präventive Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen

134 Das von den vorlegenden Gerichten und den Regierungen, die Erklärungen abgegeben haben, angesprochene Ziel des Schutzes der nationalen Sicherheit ist vom *Gerichtshof* in seinen Urteilen zur Auslegung der Richtlinie 2002/58 noch nicht spezifisch geprüft worden.

135 Insoweit ist zunächst festzustellen, dass nach Art. 4 Abs. 2 EUV die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt. Diese Verantwortung entspricht dem zentralen Anliegen, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen, und umfasst die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten.

136 Die Bedeutung des Ziels des Schutzes der nationalen Sicherheit übersteigt im Licht von Art. 4 Abs. 2 EUV 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. Bedrohungen wie die in der vorstehenden Randnummer genannten unterscheiden sich nämlich aufgrund ihrer Art und ihrer besonderen Schwere von der allgemeinen Gefahr des Auftretens selbst schwerer Spannungen oder Störungen im Bereich der öffentlichen Sicherheit. Vorbehaltlich der Erfüllung der übrigen Anforderungen von Art. 52 Abs. 1 der Charta ist das Ziel des Schutzes der nationalen Sicherheit daher geeignet, Maßnahmen zu rechtfertigen, die schwerere Grundrechtseingriffe enthalten als solche, die mit den übrigen Zielen gerechtfertigt werden könnten.

137 Somit steht Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta in Situationen wie den in den Rn. 135 und 136 des vorliegenden Urteils beschriebenen einer Rechtsvorschrift, mit der den zuständigen Behörden gestattet wird, den Betreibern elektronischer Kommunikationsdienste aufzugeben, die Verkehrs- und Standortdaten aller Nutzer elektronischer Kommunikationsmittel für begrenzte Zeit zu speichern, grundsätzlich nicht entgegen, sofern hinreichend konkrete Umstände die Annahme zulassen, dass sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit im Sinne der Rn. 135 und 136 des vorliegenden Urteils gegenübersieht. Auch wenn eine solche Maßnahme unterschiedslos alle Nutzer elektronischer Kommunikationsmittel erfasst, ohne dass *prima facie* ein Zusammenhang im Sinne der in Rn. 133 des vorliegenden Urteils angeführten Rechtsprechung zwischen ihnen und einer Bedrohung der nationalen Sicherheit dieses Mitgliedstaats zu bestehen scheint, ist gleichwohl davon auszugehen, dass das Vorliegen einer derartigen Bedrohung als solches geeignet ist, diesen Zusammenhang herzustellen.

138 Die Anordnung, die Daten aller Nutzer elektronischer Kommunikationsmittel präventiv auf Vorrat zu speichern, muss jedoch in zeitlicher Hinsicht auf das absolut Notwendige beschränkt werden. Zwar kann nicht ausgeschlossen werden, dass die an die Betreiber elektronischer Kommunikationsdienste gerichtete Anordnung, Daten auf Vorrat zu speichern, wegen des Fortbestands einer solchen Bedrohung verlängert werden kann, doch darf die Laufzeit jeder Anordnung einen absehbaren Zeitraum nicht überschreiten. Überdies muss eine solche Vorratsdatenspeicherung Beschränkungen unterliegen und mit strengen Garantien verbunden sein, die einen wirksamen Schutz der personenbezogenen Daten der Betroffenen vor Missbrauchsrisiken ermöglichen. Die Speicherung darf somit keinen systematischen Charakter haben.

139 Angesichts der Schwere des aus einer solchen allgemeinen und unterschiedslosen Speicherung resultierenden Eingriffs in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, muss gewährleistet sein, dass darauf tatsächlich nur in Situationen wie den in den Rn. 135 und 136 des vorliegenden Urteils angesprochenen zurückgegriffen wird, in denen eine ernste Bedrohung für die nationale Sicherheit besteht. Dabei ist es unabdingbar, dass eine an die Betreiber elektronischer Kommunikationsdienste gerichtete Anordnung einer solchen Vorratsdatenspeicherung Gegenstand einer wirksamen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung bindend ist, sein kann, mit der das Vorliegen einer dieser Situationen sowie die Beachtung der vorzusehenden Bedingungen und Garantien geprüft werden.

Zu den Rechtsvorschriften, die zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine präventive Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen

140 Was das 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 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 (vgl. in diesem Sinne Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 102, und Urt. v. 2.10.2018, Ministerio Fiscal, C−207/16, EU:C:2018:788, Rn. 56 und 57; Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26.7.2017, EU:C:2017:592, Rn. 149).

141 Eine nationale Regelung, die zur Bekämpfung schwerer Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, überschreitet die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta verlangt (vgl. in diesem Sinne Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 107).

142 Angesichts des sensiblen Charakters der Informationen, die sich aus den Verkehrs- und Standortdaten ergeben können, ist deren Vertraulichkeit nämlich von entscheidender Bedeutung für das Recht auf Achtung des Privatlebens. In Anbetracht zum einen der in Rn. 118 des vorliegenden Urteils angesprochenen abschreckenden Wirkungen, die die Speicherung dieser Daten auf die Ausübung der in den Art. 7 und 11 der Charta verankerten Grundrechte haben kann, und zum anderen der Schwere des mit ihr verbundenen Eingriffs muss eine solche Speicherung in einer demokratischen Gesellschaft, wie es das durch die Richtlinie 2002/58 geschaffene System vorsieht, die Ausnahme und nicht die Regel sein, und solche Daten dürfen nicht Gegenstand einer systematischen und kontinuierlichen Speicherung sein. Dies gilt auch in Anbetracht der Ziele der Bekämpfung schwerer Kriminalität und der Verhütung ernster Bedrohungen der öffentlichen Sicherheit sowie der Bedeutung, die ihnen beizumessen ist.

143 Außerdem hat der *Gerichtshof* hervorgehoben, dass eine Regelung, die eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, die elektronischen Kommunikationen fast der gesamten Bevölkerung erfasst, ohne jede Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels. Eine solche Regelung betrifft entgegen dem in Rn. 133 des vorliegenden Urteils angesprochenen Erfordernis pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt somit auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit dem Ziel der Bekämpfung schwerer Straftaten stehen könnte, und setzt insbesondere keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit voraus (vgl. in diesem Sinne Urt. v. 8.4.2014, Digital Rights, C−293/12 und C−594/12, EU:C:2014:238, Rn. 57 und 58, sowie Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 105).

144 Insbesondere beschränkt eine solche Regelung, wie der *Gerichtshof* bereits entschieden hat, die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung schwerer Kriminalität beitragen könnten (vgl. in diesem Sinne Urt. v. 8.4.2014, Digital Rights, C−293/12 und C−594/12, EU:C:2014:238, Rn. 59, und Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 106).

145 Selbst die positiven Verpflichtungen, die sich, je nach Fall, für die Mitgliedstaaten aus den Art. 3, 4 und 7 der Charta ergeben können und, wie in den Rn. 126 und 128 des vorliegenden Urteils ausgeführt worden ist, die Schaffung von Regeln für eine wirksame Bekämpfung von Straftaten betreffen, können aber keine so schwerwiegenden Eingriffe rechtfertigen, wie sie mit einer Regelung, die eine Speicherung von Verkehrs- und Standortdaten vorsieht, für die in den Art. 7 und 8 der Charta verankerten Grundrechte fast der gesamten Bevölkerung verbunden sind, ohne dass die Daten der Betroffenen einen zumindest mittelbaren Zusammenhang mit dem verfolgten Ziel aufweisen.

146 Hingegen können nach den Ausführungen in den Rn. 142 bis 144 des vorliegenden Urteils und angesichts dessen, dass die widerstreitenden Rechte und Interessen miteinander in Einklang gebracht werden müssen, die Ziele der Bekämpfung schwerer Kriminalität, der Verhütung schwerer Beeinträchtigungen der öffentlichen Sicherheit und erst recht des Schutzes der nationalen Sicherheit in Anbetracht ihrer Bedeutung im Hinblick auf die in der vorstehenden Randnummer angesprochenen positiven Verpflichtungen, auf die insbesondere der *Verfassungsgerichtshof* abgestellt hat, den mit einer gezielten Vorratsspeicherung von Verkehrs- und Standortdaten verbundenen besonders schwerwiegenden Eingriff rechtfertigen.

147 Wie der *Gerichtshof* bereits entschieden hat, untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta es einem Mitgliedstaat somit nicht, eine Regelung zu erlassen, die

zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit sowie zum Schutz der nationalen Sicherheit präventiv eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern ihre Speicherung hinsichtlich der Kategorien der zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist (vgl. in diesem Sinne Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 108).

148 Die erforderliche Begrenzung einer solchen Vorratsdatenspeicherung kann insbesondere anhand der Kategorien betroffener Personen vorgenommen werden, da Art. 15 Abs. 1 der Richtlinie 2002/58 einer auf objektiven Kriterien beruhenden Regelung nicht entgegensteht, mit der Personen erfasst werden können, deren Verkehrs- und Standortdaten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten zu offenbaren, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit oder eine Gefahr für die nationale Sicherheit zu verhüten (vgl. in diesem Sinne Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 111).

149 Insoweit ist hinzuzufügen, dass zu den erfassten Personen insbesondere diejenigen gehören können, die zuvor im Rahmen der einschlägigen nationalen Verfahren und auf der Grundlage objektiver Kriterien als Bedrohung der öffentlichen Sicherheit oder der nationalen Sicherheit des betreffenden Mitgliedstaats eingestuft wurden.

150 Die Begrenzung einer Maßnahme zur Vorratsspeicherung von Verkehrs- und Standortdaten kann auch auf ein geografisches Kriterium gestützt werden, wenn die zuständigen nationalen Behörden aufgrund objektiver und nichtdiskriminierender Anhaltspunkte davon ausgehen, dass in einem oder mehreren geografischen Gebieten eine durch ein erhöhtes Risiko der Vorbereitung oder Begehung schwerer Straftaten gekennzeichnete Situation besteht (vgl. in diesem Sinne Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 111). Dabei kann es sich insbesondere um Orte handeln, die durch eine erhöhte Zahl schwerer Straftaten gekennzeichnet sind, um Orte, an denen die Gefahr, dass schwere Straftaten begangen werden, besonders hoch ist, wie Orte oder Infrastrukturen, die regelmäßig von einer sehr hohen Zahl von Personen aufgesucht werden, oder um strategische Orte wie Flughäfen, Bahnhöfe oder Mautstellen.

151 Um sicherzustellen, dass der Eingriff, mit dem die in den Rn. 147 bis 150 des vorliegenden Urteils beschriebenen Maßnahmen gezielter Speicherung verbunden sind, mit dem Grundsatz der Verhältnismäßigkeit im Einklang steht, darf ihre Dauer das im Hinblick auf das verfolgte Ziel sowie die sie rechtfertigenden Umstände absolut Notwendige nicht überschreiten, unbeschadet einer etwaigen Verlängerung wegen des fortbestehenden Erfordernisses einer solchen Speicherung.

Zu den Rechtsvorschriften, die zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine präventive Vorratsspeicherung von IP−Adressen und die Identität betreffenden Daten vorsehen

152 IP−Adressen gehören zwar zu den Verkehrsdaten, werden aber ohne Anknüpfung an eine bestimmte Kommunikation erzeugt und dienen in erster Linie dazu, über die Betreiber elektronischer Kommunikationsdienste die natürliche Person zu ermitteln, der ein Endgerät gehört, von dem aus eine Kommunikation über das Internet stattfindet. Sofern im Bereich von E-Mail und Internettelefonie nur die IP−Adressen der Kommunikationsquelle gespeichert werden und nicht die des Adressaten einer Kommunikation, lässt sich diesen Adressen als solchen keine Information über die Dritten entnehmen, mit denen die Person, von der die Kommunikation ausging, in Kontakt stand. Diese Kategorie von Daten weist daher einen geringeren Sensibilitätsgrad als die übrigen Verkehrsdaten auf.

153 Da die IP−Adressen jedoch insbesondere zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und infolgedessen seiner Online-Aktivität genutzt werden können, ermöglichen sie die Erstellung eines detaillierten Profils dieses Nutzers. Die für eine solche Nachverfolgung erforderliche Vorratsspeicherung und Analyse der IP−Adressen stellen daher schwere Eingriffe in die Grundrechte des Internetnutzers aus den Art. 7 und 8 der Charta dar und können abschreckende Wirkungen wie die in Rn. 118 des vorliegenden Urteils dargelegten entfalten.

154 Um die widerstreitenden Rechte und Interessen miteinander in Einklang zu bringen, wie es die in Rn. 130 des vorliegenden Urteils angeführte Rechtsprechung verlangt, ist aber zu berücksichtigen, dass im Fall einer im Internet begangenen Straftat die IP−Adresse der einzige Anhaltspunkt sein kann, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde. Hinzu kommt, dass die Vorratsspeicherung der IP−Adressen durch die Betreiber elektronischer Kommunikationsdienste über die Dauer ihrer Zuweisung hinaus im Prinzip nicht erforderlich erscheint, um eine Rechnung für die fraglichen Dienste zu erstellen, so dass sich die Feststellung im Internet begangener Straftaten, wie mehrere Regierungen in ihren beim *Gerichtshof* eingereichten Erklärungen angegeben haben, ohne Rückgriff auf eine Rechtsvorschrift nach Art. 15 Abs. 1 der Richtlinie 2002/58 als unmöglich erweisen kann. Dies kann, wie diese Regierungen geltend gemacht haben, u. a. bei besonders schweren Straftaten im Bereich der Kinderpornografie im Sinne von Art. 2 Buchst. b der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. 2011, L 335, S. 1) der Fall sein, etwa wenn Kinderpornografie erworben, verbreitet, weitergegeben oder im Internet bereitgestellt wird.

155 Unter diesen Umständen trifft es zwar zu, dass eine

Rechtsvorschrift, die eine Vorratsspeicherung der IP-Adressen aller natürlichen Personen vorsieht, denen ein Endgerät gehört, von dem aus ein Internetzugang möglich ist, Personen erfassen würde, die *prima facie* keinen Zusammenhang mit den verfolgten Zielen im Sinne der in Rn. 133 des vorliegenden Urteils angeführten Rechtsprechung aufweisen, und dass die Internetnutzer nach der Feststellung in Rn. 109 des vorliegenden Urteils aufgrund der Art. 7 und 8 der Charta erwarten dürfen, dass ihre Identität grundsätzlich nicht preisgegeben wird. Gleichwohl verstößt eine Rechtsvorschrift, die eine allgemeine und unterschiedslose Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung vorsieht, grundsätzlich nicht gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta, sofern diese Möglichkeit von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig gemacht wird, die die Nutzung dieser Daten regeln müssen.

156 Angesichts der Schwere des mit dieser Vorratsdatenspeicherung verbundenen Eingriffs in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, sind neben dem Schutz der nationalen Sicherheit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet, diesen Eingriff zu rechtfertigen. Außerdem darf die Dauer der Speicherung das im Hinblick auf das verfolgte Ziel absolut Notwendige nicht überschreiten. Schließlich muss eine derartige Maßnahme strenge Voraussetzungen und Garantien hinsichtlich der Auswertung dieser Daten, insbesondere in Form einer Nachverfolgung, in Bezug auf die Online-Kommunikationen und -Aktivitäten der Betroffenen vorsehen.

157 Was schließlich die die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten angeht, ermöglichen sie es 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 wie ihren Adressen, keine Informationen über die konkreten Kommunikationen und infolgedessen über ihr Privatleben liefern. Der mit einer Vorratsspeicherung dieser Daten verbundene Eingriff kann somit grundsätzlich nicht als schwer eingestuft werden (vgl. in diesem Sinne Urt. v. 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 59 und 60).

158 Daraus ergibt sich im Einklang mit den Ausführungen in Rn. 140 des vorliegenden Urteils, dass Rechtsvorschriften, die auf die Verarbeitung dieser Daten als solcher, 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 S. 1 der Richtlinie 2002/58 genannten Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein können (vgl. in diesem Sinne Urt. v. 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 62).

159 Unter diesen Umständen ist angesichts dessen, dass die widerstreitenden Rechte und Interessen miteinander in Einklang gebracht werden müssen, aus den in den Rn. 131 und 158 des vorliegenden Urteils genannten Gründen davon auszugehen, 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, auch wenn es keine Verbindung zwischen der Gesamtheit der Nutzer elektronischer Kommunikationsmittel und den verfolgten Zielen gibt, einer Rechtsvorschrift nicht entgegensteht, die den Betreibern elektronischer Kommunikationsdienste ohne besondere Frist auferlegt, zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten sowie zum Schutz der öffentlichen Sicherheit Daten über die Identität aller Nutzer elektronischer Kommunikationsmittel auf Vorrat zu speichern, ohne dass es sich um schwere Straftaten, Bedrohungen oder Beeinträchtigungen der öffentlichen Sicherheit handeln muss.

Zu den Rechtsvorschriften, die zur Bekämpfung schwerer Kriminalität eine umgehende Sicherung von Verkehrs- und Standortdaten vorsehen

160 Die von den Betreibern elektronischer Kommunikationsdienste auf der Grundlage der Art. 5, 6 und 9 der Richtlinie 2002/58 oder auf der Grundlage von Rechtsvorschriften der in den Rn. 134 bis 159 des vorliegenden Urteils beschriebenen Art, die gemäß Art. 15 Abs. 1 der Richtlinie erlassen wurden, verarbeiteten und gespeicherten Verkehrs- und Standortdaten müssen grundsätzlich nach Ablauf der gesetzlichen Fristen, innerhalb deren sie gemäß den nationalen Bestimmungen zur Umsetzung der Richtlinie verarbeitet und gespeichert werden müssen, entweder gelöscht oder anonymisiert werden.

161 Während dieser Verarbeitung und Speicherung können jedoch Situationen auftreten, die es erforderlich machen, die betreffenden Daten zur Aufklärung schwerer Straftaten oder von Beeinträchtigungen der nationalen Sicherheit über diese Fristen hinaus zu speichern, und zwar sowohl dann, wenn die Taten oder Beeinträchtigungen bereits festgestellt werden konnten, als auch dann, wenn nach einer objektiven Prüfung aller relevanten Umstände der begründete Verdacht besteht, dass sie vorliegen.

162 Insoweit ist darauf hinzuweisen, dass das von den 27 Mitgliedstaaten unterzeichnete und von 25 von ihnen ratifizierte Übereinkommen des Europarats vom 23.11.2001 über Computerkriminalität (Sammlung Europäischer Verträge – Nr. 185), das die Bekämpfung von Straftaten, die mittels Rechnernetzen begangen wurden, erleichtern soll, in Art. 14 vorsieht, dass die Vertragsstaaten für die Zwecke spezifischer strafrechtlicher Ermittlungen oder Verfahren bestimmte Maßnahmen hinsichtlich bereits gespeicherter Verkehrsdaten treffen, zu denen die umgehende Sicherung dieser Daten gehört. Dazu heißt es in Art. 16 Abs. 1 des Übereinkommens insbesondere, dass die Vertragsparteien die erforderlichen gesetzgeberischen Maßnahmen treffen,

damit ihre zuständigen Behörden die umgehende Sicherung von Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass diese Daten verloren gehen oderverändert werden könnten.

163 In einer Situation wie der in Rn. 161 des vorliegenden Urteils beschriebenen steht es den Mitgliedstaaten angesichts dessen, dass nach den Ausführungen in Rn. 130 des vorliegenden Urteils die widerstreitenden Rechte und Interessen miteinander in Einklang gebracht werden müssen, frei, in Rechtsvorschriften, die sie gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassen, vorzusehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben wird, für einen festgelegten Zeitraum die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

164 Da die Zielsetzung einer solchen umgehenden Sicherung nicht mehr den Zielsetzungen entspricht, aufgrund deren die Daten ursprünglich gesammelt und gespeichert wurden, und da nach Art. 8 Abs. 2 der Charta jede Datenverarbeitung für festgelegte Zwecke zu erfolgen hat, müssen die Mitgliedstaaten in ihren Rechtsvorschriften angeben, mit welcher Zielsetzung die umgehende Sicherung der Daten vorgenommen werden kann. Angesichts der Schwere des Eingriffs in die Grundrechte der Art. 7 und 8 der Charta, der mit einer solchen Speicherung verbunden sein kann, sind nur die Bekämpfung schwerer Kriminalität und, *a fortiori*, der Schutz der nationalen Sicherheit geeignet, diesen Eingriff zu rechtfertigen. Um sicherzustellen, dass der mit einer derartigen Maßnahme verbundene Eingriff auf das absolut Notwendige beschränkt bleibt, darf sich die Speicherungspflicht zudem zum einen nur auf Verkehrs- und Standortdaten erstrecken, die zur Aufdeckung der schweren Straftat oder der Beeinträchtigung der nationalen Sicherheit beitragen können. Zum anderen muss die Speicherungsdauer der Daten auf das absolut Notwendige beschränkt bleiben, kann allerdings verlängert werden, wenn die Umstände und das mit der fraglichen Maßnahme verfolgte Ziel es rechtfertigen.

165 Insoweit ist hinzuzufügen, dass sich eine solche umgehende Sicherung nicht auf die Daten der Personen beschränken muss, die konkret im Verdacht stehen, eine Straftat begangen oder die nationale Sicherheit beeinträchtigt zu haben. Unter Beachtung des durch Art. 15 Abs.1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta vorgegebenen Rahmens und angesichts der Erwägungen in Rn. 133 des vorliegenden Urteils kann eine solche Maßnahme nach Wahl des Gesetzgebers, unter Einhaltung der Grenzen des absolut Notwendigen, auf die Verkehrs- und Standortdaten anderer als der Personen erstreckt werden, die im Verdacht stehen, eine schwere Straftat oder eine Beeinträchtigung der nationalen Sicherheit geplant oder begangen zu haben, sofern diese Daten auf der Grundlage objektiver und nicht diskriminierender Kriterien zur Aufdeckung einer solchen Straftat oder einer solchen Beeinträchtigung der nationalen Sicherheit beitragen können. Dazu gehören die Daten des Opfers, seines sozialen oder beruflichen Umfelds oder bestimmter geografischer Zonen, etwa der Orte, an denen die fragliche Straftat oder Beeinträchtigung der nationalen Sicherheit begangen oder vorbereitet wurde. Außerdem müssen beim Zugang der zuständigen Behörden zu den gespeicherten Daten die Voraussetzungen eingehalten werden, die sich aus der Rechtsprechung zur Auslegung der Richtlinie 2002/58 ergeben (vgl. in diesem Sinne Urt. v. 21.12.2016, Tele2, C−203/15 und C−698/15, EU:C:2016:970, Rn. 118 bis 121 und die dort angeführte Rechtsprechung).

166 Ferner ist hinzuzufügen, dass – wie sich insbesondere aus den Rn. 115 und 133 des vorliegenden Urteils ergibt – der Zugang zu den von den Betreibern elektronischer Kommunikationsdienste in Anwendung einer gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassenen Rechtsvorschrift gespeicherten Verkehrs- und Standortdaten grundsätzlich nur mit dem dem Gemeinwohl dienenden Ziel gerechtfertigt werden kann, zu dem die Speicherung den Betreibern auferlegt wurde. Daraus folgt insbesondere, dass keinesfalls ein Zugang zu solchen Daten zwecks Verfolgung und Ahndung einer gewöhnlichen Straftat gewährt werden kann, wenn ihre Speicherung mit dem Ziel der Bekämpfung schwerer Kriminalität oder gar dem Schutz der nationalen Sicherheit gerechtfertigt wurde. Dagegen kann, im Einklang mit dem Grundsatz der Verhältnismäßigkeit nach seiner Auslegung in Rn. 131 des vorliegenden Urteils, ein Zugang zu Daten, die im Hinblick auf die Bekämpfung schwerer Kriminalität gespeichert wurden, mit dem Ziel des Schutzes der nationalen Sicherheit gerechtfertigt werden, sofern die in der vorstehenden Randnummer genannten materiellen und prozeduralen Voraussetzungen für einen solchen Zugang eingehalten werden.

167 Insoweit steht es den Mitgliedstaaten frei, in ihren Rechtsvorschriften vorzusehen, dass ein Zugang zu Verkehrs- und Standortdaten bei Einhaltung der fraglichen materiellen und prozeduralen Voraussetzungen zur Bekämpfung schwerer Kriminalität oder zum Schutz der nationalen Sicherheit erfolgen kann, wenn diese Daten von einem Betreiber in einer mit den Art. 5, 6 und 9 oder mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Einklang stehenden Weise gespeichert wurden.

168 Nach alledem ist auf die erste Frage in den Rechtssachen C−511/18 und C−512/18 sowie auf die erste und die zweite Frage in der Rechtssache C−520/18 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 Rechtsvorschriften entgegensteht, die zu den in Art. 15 Abs. 1 genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Dagegen steht Art. 15 Abs. 1 der Richtlinie im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta Rechtsvorschriften nicht entgegen, die

- es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste

aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht;

- zum Schutz der nationalen Sicherheit, 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;
- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;
- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen
- es zur Bekämpfung schwerer Kriminalität und, *a fortiori*, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung 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.

Zur zweiten und zur dritten Frage in der Rechtssache C-511/18

169 Mit seiner zweiten und seiner dritten Frage in der Rechtssache C-511/18 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, mit der den Betreibern elektronischer Kommunikationsdienste aufgegeben wird, in ihren Netzen Maßnahmen umzusetzen, die es ermöglichen, zum einen Verkehrs- und Standortdaten automatisiert zu analysieren und in Echtzeit zu erheben und zum anderen die technischen Daten zum Standort der verwendeten Endgeräte in Echtzeit zu erheben, ohne dass die Unterrichtung der Betroffenen von diesen Verarbeitungen und Datenerhebungen vorgesehen ist.

170 Das vorlegende Gericht führt aus, die in den Art. L. 851-2 bis L. 851-4 des CSI vorgesehenen Techniken zur Gewinnung nachrichtendienstlicher Erkenntnisse seien für die Betreiber elektronischer Kommunikationsdienste nicht mit einem spezifischen Erfordernis der Vorratsspeicherung von Verkehrs- und Standortdaten verbunden. Insbesondere sollten mit der in Art. L. 851-3 des CSI geregelten automatisierten Analyse anhand von dafür festgelegten Kriterien Verbindungen aufgespürt werden, die auf eine terroristische Bedrohung hindeuten könnten. Die in Art. L. 851-2 des CSI geregelte Erhebung in Echtzeit betreffe nur eine oder mehrere Personen, von denen zuvor festgestellt worden sei, dass sie mit einer terroristischen Bedrohung in Zusammenhang stehen könnten. Diese beiden Techniken könnten nur zur Verhütung des Terrorismus eingesetzt werden und beträfen die von den Art. L. 851-1 und R. 851-5 des CSI erfassten Daten.

171 Zunächst ist darauf hinzuweisen, dass der Umstand, dass nach Art. L. 851-3 des CSI die dort vorgesehene automatisierte Analyse es als solche nicht ermöglicht, die Nutzer zu identifizieren, deren Daten dieser Analyse unterzogen werden, der Einstufung solcher Daten als „personenbezogene Daten“ nicht entgegensteht. Da das in Abschnitt IV dieser Bestimmung vorgesehene Verfahren es gestattet, die Personen, bei denen die automatisierte Analyse ihrer Daten ergeben hat, dass eine terroristische Bedrohung vorliegen kann, später zu identifizieren, bleiben nämlich alle Personen, deren Daten Gegenstand der automatisierten Analyse waren, anhand dieser Daten identifizierbar. Nach der Definition in Art. 4 Nr. 1 der Verordnung 2016/679 sind aber u. a. Informationen, die sich auf eine identifizierbare Person beziehen, personenbezogene Daten.

Zur automatisierten Analyse von Verkehrs- und Standortdaten

172 Wie aus Art. L. 851-3 des CSI hervorgeht, entspricht die dort vorgesehene automatisierte Analyse im Wesentlichen einer Filterung aller von den Betreibern elektronischer Kommunikationsdienste gespeicherten Verkehrs- und Standortdaten, die von ihnen auf Ersuchen der zuständigen nationalen Behörden in Anwendung der von diesen festgelegten Parametern vorgenommen wird. Daraus folgt, dass alle Daten der Nutzer elektronischer Kommunikationsmittel daraufhin überprüft werden, ob sie diesen Parametern entsprechen. Daher ist davon auszugehen, dass eine solche automatisierte Analyse für die Betreiber elektronischer Kommunikationsdienste darin besteht, für die zuständige Behörde eine allgemeine und unterschiedslose Verarbeitung vorzunehmen, die alle Verkehrs- und

Standortdaten aller Nutzer elektronischer Kommunikationsmittel erfasst und in einer Nutzung der Daten mit Hilfe eines automatisierten Verfahrens im Sinne von Art. 4 Nr. 2 der Verordnung 2016/679 besteht. Diese Verarbeitung ist von der späteren, nach Abschnitt IV von Art. L. 851-3 des CSI zulässigen Erhebung der Daten der Personen, die im Anschluss an die automatisierte Analyse identifiziert wurden, unabhängig.

173 Eine nationale Regelung, die eine solche automatisierte Analyse der Verkehrs- und Standortdaten gestattet, weicht aber von der grundsätzlichen, in Art. 5 der Richtlinie 2002/58 aufgestellten Pflicht ab, die Vertraulichkeit der elektronischen Kommunikation und der damit verbundenen Daten sicherzustellen. Eine solche Regelung greift auch, unabhängig davon, wie diese Daten später genutzt werden, in die Grundrechte ein, die in den Art. 7 und 8 der Charta verankert sind. Schließlich kann sie im Sinne der in Rn. 118 des vorliegenden Urteils angeführten Rechtsprechung abschreckende Wirkungen in Bezug auf die Ausübung der durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung entfalten.

174 Überdies ist der aus einer automatisierten Analyse der Verkehrs- und Standortdaten wie der im Ausgangsverfahren in Rede stehenden resultierende Eingriff besonders schwerwiegend, da sie sich allgemein und unterschiedslos auf die Daten der Nutzer elektronischer Kommunikationsmittel erstreckt. Dies gilt umso mehr, als sich den Daten, die Gegenstand der automatisierten Analyse sind, die Art der im Internet konsultierten Informationen entnehmen lässt, wie aus der im Ausgangsverfahren in Rede stehenden nationalen Regelung hervorgeht. Außerdem wird eine solche automatisierte Analyse global bei allen Nutzern elektronischer Kommunikationsmittel vorgenommen, also auch bei Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit terroristischen Aktivitäten stehen könnte.

175 Zur Rechtfertigung eines solchen Eingriffs ist festzustellen, dass das in Art. 52 Abs. 1 der Charta aufgestellte Erfordernis einer gesetzlichen Grundlage für jede Einschränkung der Ausübung von Grundrechten bedeutet, dass die gesetzliche Grundlage für den Eingriff selbst festlegen muss, in welchem Umfang die Ausübung des betreffenden Rechts eingeschränkt wird (vgl. in diesem Sinne Urteil vom 16. Juli 2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559, Rn. 175 und die dort angeführte Rechtsprechung).

176 Um dem in den Rn. 130 und 131 des vorliegenden Urteils angesprochenen Erfordernis der Verhältnismäßigkeit, wonach Ausnahmen vom Schutz personenbezogener Daten und dessen Beschränkungen nicht über das absolut Notwendige hinausgehen dürfen, zu genügen, muss eine nationale Regelung des Zugangs der zuständigen Behörden zu den gespeicherten Verkehrs- und Standortdaten zudem den Anforderungen entsprechen, die sich aus der in Rn. 132 des vorliegenden Urteils angeführten Rechtsprechung ergeben. Eine solche Regelung darf sich insbesondere 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 (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU– Kanada] vom 26.7.2017, EU:C:2017:592, Rn. 192 und die dort angeführte Rechtsprechung).

177 Insoweit ist darauf hinzuweisen, dass der mit einer allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten verbundene besonders schwere Eingriff, auf den sich die Erwägungen in den Rn. 134 bis 139 des vorliegenden Urteils beziehen, sowie der besonders schwere Eingriff in Form ihrer automatisierten Analyse dem Erfordernis der Verhältnismäßigkeit nur in Situationen genügen kann, in denen sich ein Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, und nur unter der Voraussetzung, dass sich die Dauer dieser Speicherung auf das absolut Notwendige beschränkt.

178 In Situationen wie den in der vorstehenden Randnummer angesprochenen kann eine automatisierte Analyse der Verkehrs- und Standortdaten aller Nutzer elektronischer Kommunikationsmittel während eines streng begrenzten Zeitraums im Hinblick auf die Anforderungen, die sich aus Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta ergeben, als gerechtfertigt angesehen werden.

179 Um sicherzustellen, dass sich der Rückgriff auf eine solche Maßnahme tatsächlich auf das zum Schutz der nationalen Sicherheit und insbesondere zur Verhütung des Terrorismus absolut Notwendige beschränkt, ist es nach den Feststellungen in Rn. 139 des vorliegenden Urteils allerdings unabdingbar, dass die Entscheidung, mit der die automatisierte Analyse gestattet wird, Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer die fragliche Maßnahme rechtfertigenden Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist.

180 Insoweit ist hinzuzufügen, dass die im Voraus festgelegten Modelle und Kriterien, auf denen diese Art der Datenverarbeitung beruht, zum einen spezifisch und zuverlässig sein müssen, so dass sie zu Ergebnissen führen, die es ermöglichen, Personen zu identifizieren, gegen die ein begründeter Verdacht der Beteiligung an terroristischen Straftaten bestehen könnte, und zum anderen nicht diskriminierend sein dürfen (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26.7.2017, EU:C:2017:592, Rn. 172).

181 Außerdem ist darauf hinzuweisen, dass jede automatisierte Analyse anhand von Modellen und Kriterien, die auf dem Postulat beruhen, dass die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, der Gesundheitszustand oder das Sexualleben ei-

ner Person als solche, unabhängig vom konkreten Verhalten dieser Person, für die Verhütung des Terrorismus relevant sein könnten, gegen die in den Art. 7 und 8 der Charta in Verbindung mit deren Art. 21 garantierten Rechte verstoßen würde. Die für eine automatisierte Analyse, mit der terroristische Aktivitäten verhindert werden sollen, die eine ernste Bedrohung für die nationale Sicherheit darstellen, im Voraus festgelegten Modelle und Kriterien dürfen daher nicht allein auf diesen sensiblen Daten beruhen (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26.7.2017, EU:C:2017:592, Rn. 165).

182 Da die automatisierten Analysen der Verkehrs- und Standortdaten zwangsläufig eine gewisse Fehlerquote aufweisen, muss jedes positive Ergebnis, das durch eine automatisierte Verarbeitung erlangt wurde, überdies individuell mit nicht automatisierten Mitteln wie der anschließenden Erhebung von Verkehrs- und Standortdaten in Echtzeit überprüft werden, bevor eine individuelle Maßnahme mit nachteiligen Auswirkungen auf die betreffenden Personen getroffen wird. Eine solche Maßnahme darf nämlich nicht allein auf dem Ergebnis einer automatisierten Verarbeitung beruhen. Desgleichen müssen, um in der Praxis zu gewährleisten, dass die im Voraus festgelegten Modelle und Kriterien, deren Anwendung sowie die verwendeten Datenbanken nicht diskriminierend sind und sich im Hinblick auf das Ziel, terroristische Aktivitäten zu verhindern, die´eine ernste Bedrohung für die nationale Sicherheit darstellen, auf das absolut Notwendige beschränken, die Zuverlässigkeit und Aktualität dieser Modelle und Kriterien sowie der verwendeten Datenbanken regelmäßig überprüft werden (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26.7.2017, EU:C:2017:592, Rn. 173 und 174).

Zur Erhebung von Verkehrs- und Standortdaten in Echtzeit

183 Zu der in Art. L. 851-2 des CSI geregelten Erhebung von Verkehrs- und Standortdaten in Echtzeit ist festzustellen, dass sie in Bezug auf „eine Person, von der zuvor festgestellt wurde, dass sie verdächtigt wird, in Verbindung mit einer [terroristischen] Bedrohung zu stehen", individuell genehmigt werden kann. Weiter heißt es in dieser Bestimmung: „Bestehen schwerwiegende Gründe für die Annahme, dass eine oder mehrere Personen aus dem Umfeld der Person, auf die sich die Genehmigung bezieht, Informationen im Zusammenhang mit der Zielsetzung, auf der die Genehmigung beruht, liefern können, kann sie auch individuell für jede dieser Personen vorgenommen werden."

184 Die Daten, die Gegenstand einer derartigen Maßnahme sind, ermöglichen es den zuständigen nationalen Behörden, für die Dauer der Genehmigung kontinuierlich und in Echtzeit zu überwachen, mit wem die betreffenden Personen kommunizieren, welche Mittel sie verwenden, wie lange ihre Kommunikationen dauern, wo sich die Personen aufhalten und wohin sie sich begeben. Desgleichen lässt sich ihnen offenbar die Art der online konsultierten Informationen entnehmen. Aus der Gesamtheit dieser Daten können, wie sich aus Rn. 117 des vorliegenden Urteils ergibt, sehr genaue Schlüsse auf das Privatleben der betreffenden Personen gezogen werden, und sie ermöglichen die Erstellung eines Profils der Betroffenen, das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible Information darstellt wie der Inhalt der Kommunikationen selbst.

185 Die in Art. L. 851-4 des CSI geregelte Erhebung von Daten in Echtzeit gestattet es, technische Daten über die Standorte der Endgeräte zu erheben und in Echtzeit einer Dienststelle des Premierministers zu übermitteln. Solche Daten ermöglichen es der zuständigen Dienststelle offenbar, für die Dauer der Genehmigung jederzeit kontinuierlich und in Echtzeit den Standort der verwendeten Endgeräte, etwa von Mobiltelefonen, zu bestimmen.

186 Eine nationale Regelung, die solche Erhebungen in Echtzeit gestattet, weicht wie die Regelung, die eine automatisierte Datenanalyse gestattet, von der grundsätzlichen, in Art. 5 der Richtlinie 2002/58 aufgestellten Pflicht ab, die Vertraulichkeit der elektronischen Kommunikation und der damit verbundenen Daten sicherzustellen. Sie greift daher ebenfalls in die Grundrechte ein, die in den Art. 7 und 8 der Charta verankert sind, und kann abschreckende Wirkungen in Bezug auf die Ausübung der durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung entfalten.

187 Der Eingriff, der mit einer Erhebung von Daten, die es ermöglichen, den Standort eines Endgeräts zu ermitteln, in Echtzeit verbunden ist, ist besonders schwerwiegend, denn diese Daten versetzen die zuständigen nationalen Behörden in die Lage, die Ortsveränderungen der Nutzer von Mobiltelefonen präzise und permanent nachzuverfolgen. Da diese Daten somit als besonders sensibel einzustufen sind, ist der Echtzeit-Zugang der zuständigen Behörden zu solchen Daten von einem zeitversetzten Zugang zu ihnen zu unterscheiden; Ersterer ist einschneidender, weil er eine nahezu perfekte Überwachung dieser Nutzer erlaubt (vgl. entsprechend, in Bezug auf Art. 8 der EMRK, *EGMR*, Urt. v. 8.2.2018, Ben Faiza gegen Frankreich, CE:ECHR:2018:0208JUD003144612, § 74). Die Schwere dieses Eingriffs ist noch größer, wenn sich die Erhebung in Echtzeit auch auf die Verkehrsdaten der betreffenden Personen erstreckt.

188 Das Ziel der Verhütung des Terrorismus, das mit der im Ausgangsverfahren in Rede stehenden nationalen Regelung verfolgt wird, vermag zwar angesichts seiner Bedeutung den mit der Erhebung von Verkehrs- und Standortdaten in Echtzeit verbundenen Eingriff zu rechtfertigen, doch darf eine solche Maßnahme aufgrund ihres besonders eingriffsintensiven Charakters nur bei Personen angewandt werden, bei denen ein triftiger Grund für den Verdacht besteht, dass sie auf irgendeine Weise in terroristische Aktivitäten verwickelt sind. Die Daten von Personen, die nicht zu dieser Gruppe gehören, dürfen nur Gegenstand eines zeitversetzten Zugangs sein, der nach der Rechtsprechung des *Gerichtshofs* nur in besonderen Situationen wie etwa solchen, in denen es um terroristische Aktivitäten geht, gewährt werden darf und nur dann, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in

einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung des Terrorismus leisten könnten (vgl. in diesem Sinne Urt. v. 21.12.2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 119 und die dort angeführte Rechtsprechung).

189 Außerdem muss eine Entscheidung, mit der die Erhebung von Verkehrs- und Standortdaten in Echtzeit gestattet wird, auf objektiven, in den nationalen Rechtsvorschriften vorgesehenen Kriterien beruhen. Insbesondere müssen in diesen Rechtsvorschriften nach der in Rn. 176 des vorliegenden Urteils angeführten Rechtsprechung die Umstände und Voraussetzungen festgelegt werden, unter denen eine solche Datenerhebung gestattet werden kann, und sie müssen, wie in der vorstehenden Randnummer dargelegt, vorsehen, dass nur Personen erfasst werden dürfen, bei denen eine Verbindung zu dem Ziel der Verhütung des Terrorismus besteht. Ferner muss eine Entscheidung, mit der die Erhebung von Verkehrs- und Standortdaten in Echtzeit gestattet wird, auf objektiven und nicht diskriminierenden, in den nationalen Rechtsvorschriften vorgesehenen Kriterien beruhen. Um in der Praxis die Einhaltung dieser Voraussetzungen zu gewährleisten, ist es unabdingbar, dass die Umsetzung der Maßnahme, mit der die Erhebung in Echtzeit gestattet wird, einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird, deren Entscheidung bindend ist; dieses Gericht oder diese Stelle muss sich insbesondere vergewissern, dass eine solche Erhebung in Echtzeit nur in den Grenzen des absolut Notwendigen gestattet wird (vgl. in diesem Sinne Urt. v. 21.12.2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 120). In hinreichend begründeten Eilfällen muss die Kontrolle kurzfristig erfolgen.

Zur Unterrichtung der Personen, deren Daten erhoben oder analysiert wurden

190 Die zuständigen nationalen Behörden, die Verkehrs- und Standortdaten in Echtzeit erheben, müssen die betroffenen Personen im Rahmen der einschlägigen nationalen Verfahren davon unterrichten, sofern und sobald ihre Unterrichtung die Aufgaben, mit denen diese Behörden betraut sind, nicht beeinträchtigen kann. Diese Unterrichtung ist nämlich der Sache nach erforderlich, damit die betroffenen Personen ihre Rechte aus den Art. 7 und 8 der Charta ausüben, Zugang zu ihren personenbezogenen Daten, die Gegenstand dieser Maßnahmen sind, beantragen und gegebenenfalls die Berichtigung oder Löschung dieser Daten verlangen sowie gemäß Art. 47 Abs. 1 der Charta einen wirksamen Rechtsbehelf bei einem Gericht einlegen können. Ein solches Recht wird im Übrigen durch Art. 15 Abs. 2 der Richtlinie 2002/58 in Verbindung mit Art. 79 Abs. 1 der Verordnung 2016/679 ausdrücklich gewährleistet (vgl. in diesem Sinne Urt. v. 21.12.2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 121 und die dort angeführte Rechtsprechung, sowie Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26.7.2017, EU:C:2017:592, Rn. 219 und 220).

191 Was die erforderliche Unterrichtung im Kontext einer automatisierten Analyse von Verkehrs- und Standortdaten angeht, ist die zuständige nationale Behörde verpflichtet, Informationen allgemeiner Art über diese Analyse zu veröffentlichen, ohne die Betroffenen individuell unterrichten zu müssen. Falls die Daten den in der Maßnahme, mit der die automatisierte Analyse gestattet wird, angegebenen Parametern entsprechen und die Behörde die fragliche Person identifiziert, um die sie betreffenden Daten eingehender zu analysieren, ist hingegen ihre individuelle Unterrichtung erforderlich. Eine solche Unterrichtung muss jedoch nur erfolgen, sofern und sobald sie die Aufgaben, mit denen die betreffende Behörde betraut ist, nicht beeinträchtigen kann (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26.7.2017, EU:C:2017:592, Rn. 222 bis 224).

192 Nach alledem ist auf die zweite und die dritte Frage in der Rechtssache C-511/18 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 nicht entgegensteht, mit der den Betreibern elektronischer Kommunikationsdienste auferlegt wird, zum einen eine automatisierte Analyse sowie eine Erhebung in Echtzeit insbesondere von Verkehrs- und Standortdaten und zum anderen eine Erhebung in Echtzeit der technischen Daten zum Standort der verwendeten Endgeräte vorzunehmen, sofern

- der Rückgriff auf die automatisierte Analyse auf Situationen beschränkt ist, in denen sich ein Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, und Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer die fragliche Maßnahme rechtfertigenden Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und
- der Rückgriff auf die Erhebung von Verkehrs- und Standortdaten in Echtzeit auf Personen beschränkt ist, bei denen ein triftiger Grund für den Verdacht besteht, dass sie auf irgendeine Weise in terroristische Aktivitäten verwickelt sind, und einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegt, deren Entscheidung bindend ist, wobei dieses Gericht oder diese Stelle sich vergewissern muss, dass eine solche Erhebung in Echtzeit nur in den Grenzen des absolut Notwendigen gestattet wird. In hinreichend begründeten Eilfällen muss die Kontrolle kurzfristig erfolgen.

Zur zweiten Frage in der Rechtssache C-512/18

193 Mit der zweiten Frage in der Rechtssache C-512/18 möchte das vorlegende Gericht wissen, ob die Bestimmungen der Richtlinie 2000/31 im Licht der Art. 6 bis 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen sind, dass sie einer nationalen Regelung entgegenstehen, mit der den Anbietern eines öffentlichen Online-Zugangs zu Kommunikationsdiensten und den Betreibern von Hosting-Diensten eine allgemeine und unterschieds-

lose Vorratsspeicherung insbesondere von personenbezogenen Daten im Zusammenhang mit diesen Diensten auferlegt wird.

194 Das vorlegende Gericht ist der Meinung, dass solche Dienste unter die Richtlinie 2000/31 fielen und nicht unter die Richtlinie 2002/58 und dass Art. 15 Abs. 1 und 2 der Richtlinie 2000/31 in Verbindung mit ihren Art. 12 und 14 für sich genommen kein grundsätzliches Verbot der Speicherung von Daten in Bezug auf die Schaffung von Inhalten aufstelle, von dem nur ausnahmsweise abgewichen werden könnte. Fraglich sei jedoch, ob in Anbetracht dessen, dass die in den Art. 6 bis 8 und 11 der Charta verankerten Grundrechte beachtet werden müssten, an dieser Beurteilung festzuhalten sei.

195 Das vorlegende Gericht fügt hinzu, seine Frage betreffe die in Art. 6 der LCEN in Verbindung mit dem Dekret Nr. 2011-219 vorgesehene Speicherungspflicht. Zu den Daten, die die Anbieter der betreffenden Dienste insoweit auf Vorrat speichern müssten, gehörten u.a. Daten zur Identität der Nutzer dieser Dienste wie ihre Namen, Vornamen, Postanschriften, E-Mail- oder Kontoadressen und Passwörter sowie, wenn der Abschluss des Vertrags oder die Einrichtung des Kontos kostenpflichtig sei, die verwendete Zahlungsart, die Zahlungsreferenz, der Betrag sowie Datum und Uhrzeit der Transaktion.

196 Desgleichen erstreckten sich die von der Pflicht zur Vorratsspeicherung erfassten Daten auf die Kennungen der Teilnehmer, der Verbindungen und der verwendeten Endgeräte, die den Inhalten zugewiesenen Kennungen, Datum und Uhrzeit von Beginn und Ende der Verbindungen und Vorgänge sowie die Arten der für die Verbindung zum Dienst und für die Übertragung der Inhalte verwendeten Protokolle. Der Zugang zu diesen Daten, die ein Jahr lang zu speichern seien, könne im Rahmen von Straf- und Zivilverfahren beantragt werden, um für die Beachtung der Vorschriften über die zivil- oder strafrechtliche Haftung zu sorgen, sowie im Rahmen von Maßnahmen zur Sammlung nachrichtendienstlicher Erkenntnisse, für die Art. L. 851-1 des CSI gelte.

197 Hierzu ist festzustellen, dass die Richtlinie 2000/31 nach ihrem Art. 1 Abs. 2 für eine Angleichung bestimmter für die Dienste der Informationsgesellschaft im Sinne ihres Art. 2 Buchst. a geltender innerstaatlicher Regelungen sorgt.

198 Zu solchen Diensten gehören zwar diejenigen, die im Fernabsatz mittels Geräten für die elektronische Verarbeitung und Speicherung von Daten auf individuellen Abruf eines Diensteempfängers und in der Regel gegen Entgelt erbracht werden, wie Dienste für den Zugang zum Internet oder zu einem Kommunikationsnetz sowie Hosting-Dienste (vgl. in diesem Sinne Urt. v. 24.11.2011, Scarlet Extended, C-70/10, EU:C:2011:771, Rn. 40; Urt. v. 16.2.2012, SABAM, C-360/10, EU:C:2012:85, Rn. 34; Urt. v. 15.9.2016, Mc Fadden, C-484/14, EU:C:2016:689, Rn. 55; und Urt. v. 7.8.2018, SNB-REACT, C-521/17, EU:C:2018:639, Rn. 42 und die dort angeführte Rechtsprechung).

199 Nach ihrem Art. 1 Abs. 5 findet die Richtlinie 2000/31 jedoch keine Anwendung auf Fragen betreffend die Dienste der Informationsgesellschaft, die von den Richtlinien 95/46 und 97/66 erfasst werden. Insoweit ergibt sich aus den Erwägungsgründen 14 und 15 der Richtlinie 2000/31, dass der Schutz der Vertraulichkeit der Kommunikation sowie der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Rahmen der Dienste der Informationsgesellschaft ausschließlich Gegenstand der Richtlinien 95/46 und 97/66 sind. Letztere verbietet in ihrem Art. 5 zum Schutz der Vertraulichkeit der Kommunikation jede Art des Abfangens oder Überwachens der Kommunikation.

200 Fragen, die mit dem Schutz der Vertraulichkeit der Kommunikation und personenbezogener Daten zusammenhängen, sind daher anhand der Richtlinie 2002/58 und der Verordnung 2016/679 zu beurteilen, die an die Stelle der Richtlinie 97/66 bzw. der Richtlinie 95/46 getreten sind, wobei der Schutz, den die Richtlinie 2000/31 gewährleisten soll, auf keinen Fall die Erfordernisse, die sich aus der Richtlinie 2002/58 und der Verordnung 2016/679 ergeben, beeinträchtigen darf (vgl. in diesem Sinne Urt. v. 29.1.2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 57).

201 Die Pflicht zur Vorratsspeicherung, die den Anbietern eines öffentlichen Online-Zugangs zu Kommunikationsdiensten und den Betreibern von Hosting-Diensten durch die in Rn. 195 des vorliegenden Urteils angesprochene nationale Regelung in Bezug auf die mit diesen Diensten verbundenen personenbezogenen Daten auferlegt wird, muss daher, wie der Generalanwalt im Wesentlichen in Nr. 141 seiner Schlussanträge in den verbundenen Rechtssachen La Quadrature du Net u. a. (C-511/18 und C-512/18, EU:C:2020:6) ausgeführt hat, anhand der Richtlinie 2002/58 oder der Verordnung 2016/679 beurteilt werden.

202 Je nachdem, ob die Erbringung der von dieser nationalen Regelung erfassten Dienste unter die Richtlinie 2002/58 fällt oder nicht, gilt für sie daher entweder diese Richtlinie, insbesondere ihr Art. 15 Abs. 1 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta, oder die Verordnung 2016/679, insbesondere ihr Art. 23 Abs. 1 im Licht der gleichen Bestimmungen der Charta.

203 Im vorliegenden Fall kann, wie die Europäische Kommission in ihren schriftlichen Erklärungen ausgeführt hat, nicht ausgeschlossen werden, dass einige der Dienste, auf die die in Rn. 195 des vorliegenden Urteils angesprochene nationale Regelung Anwendung findet, elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/58 darstellen; dies zu prüfen ist Sache des vorlegenden Gerichts.

204 Hierzu ist festzustellen, dass die Richtlinie 2002/58 elektronische Kommunikationsdienste erfasst, die die in Art. 2 Buchst. c der Richtlinie 2002/21, auf den Art. 2 der Richtlinie 2002/58 Bezug nimmt, aufgestellten Voraussetzungen erfüllen; dort werden elektronische Kommunikationsdienste definiert als „gewöhnlich gegen Entgelt erbrachte

Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen“. Die von der Richtlinie 2000/31 erfassten Dienste der Informationsgesellschaft im Sinne der Rn. 197 und 198 des vorliegenden Urteils stellen elektronische Kommunikationsdienste dar, wenn sie ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen (vgl. in diesem Sinne Urt. v. 5.6.2019, Skype Communications, C-142/18, EU:C:2019:460, Rn. 47 und 48).

205 Die Internetzugangsdienste, die offenbar von der in Rn. 195 des vorliegenden Urteils angesprochenen nationalen Regelung erfasst werden, stellen somit, wie der zehnte Erwägungsgrund der Richtlinie 2002/21 bestätigt, elektronische Kommunikationsdienste im Sinne dieser Richtlinie dar (vgl. in diesem Sinne Urt. v. 5.6.2019, Skype Communications, C-142/18, EU:C:2019:460, Rn. 37). Dies gilt auch für die möglicherweise ebenfalls unter diese nationale Regelung fallenden internetbasierten E-Mail-Dienste, wenn sie in technischer Hinsicht ganz oder überwiegend die Übertragung von Signalen über elektronische Kommunikationsnetze implizieren (vgl. in diesem Sinne Urt. v. 13.6.2019, Google, C-193/18, EU:C:2019:498, Rn. 35 und 38).

206 Hinsichtlich der Erfordernisse, die sich aus Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta ergeben, ist auf die gesamten Feststellungen und Erwägungen im Rahmen der Antwort auf die erste Frage in den Rechtssachen C-511/18 und C-512/18 sowie auf die erste und die zweite Frage in der Rechtssache C-520/18 zu verweisen.

207 In Bezug auf die Erfordernisse, die sich aus der Verordnung 2016/679 ergeben, ist darauf hinzuweisen, dass sie, wie sich aus ihrem zehnten Erwägungsgrund ergibt, namentlich darauf abzielt, innerhalb der Union ein hohes Datenschutzniveau für natürliche Personen zu gewährleisten und zu diesem Zweck für eine unionsweit gleichmäßige und einheitliche Anwendung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten dieser Personen bei der Verarbeitung personenbezogener Daten zu sorgen (vgl. in diesem Sinne Urt. v. 16.7.2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559, Rn. 101).

208 Zu diesem Zweck müssen bei jeder Verarbeitung personenbezogener Daten, vorbehaltlich der nach Art. 23 der Verordnung 2016/679 zulässigen Ausnahmen, die in ihrem Kapitel II aufgestellten Grundsätze für die Verarbeitung personenbezogener Daten sowie die in ihrem Kapitel III geregelten Rechte der betroffenen Person beachtet werden. Insbesondere muss jede Verarbeitung personenbezogener Daten zum einen mit den in Art. 5 der Verordnung aufgestellten Grundsätzen im Einklang stehen und zum anderen die in Art. 6 der Verordnung aufgezählten Rechtmäßigkeitsvoraussetzungen erfüllen (vgl. entsprechend, in Bezug auf die Richtlinie 95/46, Urt. v. 30.5.2013, Worten, C-342/12, EU:C:2013:355, Rn. 33 und die dort angeführte Rechtsprechung).

209 Speziell zu Art. 23 Abs. 1 der Verordnung 2016/679 ist festzustellen, dass er es, wie Art. 15 Abs. 1 der Richtlinie 2002/58, den Mitgliedstaaten gestattet, im Hinblick auf die Ziele, die er vorsieht, und mittels Gesetzgebungsmaßnahmen die dort genannten Pflichten und Rechte zu beschränken, „sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die [das verfolgte Ziel] sicherstellt“. Jede auf dieser Grundlage getroffene Gesetzgebungsmaßnahme muss insbesondere den in Art. 23 Abs. 2 der Verordnung aufgestellten spezifischen Anforderungen genügen.

210 Art. 23 Abs. 1 und 2 der Verordnung 2016/679 kann somit nicht dahin ausgelegt werden, dass er den Mitgliedstaaten die Befugnis zu einer Beeinträchtigung der Achtung des Privatlebens, unter Verstoß gegen Art. 7 der Charta, oder der übrigen in der Charta vorgesehenen Garantien verleihen kann (vgl. entsprechend, in Bezug auf die Richtlinie 95/46, Urt. v. 20.5.2003, Österreichischer Rundfunk u.a., C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 91). Insbesondere darf, ebenso wie bei Art. 15 Abs. 1 der Richtlinie 2002/58, die den Mitgliedstaaten durch Art. 23 Abs. 1 der Verordnung 2016/679 verliehene Befugnis nur unter Wahrung des Erfordernisses der Verhältnismäßigkeit ausgeübt werden, wonach Ausnahmen vom Schutz personenbezogener Daten und dessen Beschränkungen nicht über das absolut Notwendige hinausgehen dürfen (vgl. entsprechend, in Bezug auf die Richtlinie 95/46, Urt. v. 7. 11.2013, IPI, C-473/12, EU:C:2013:715, Rn. 39 und die dort angeführte Rechtsprechung).

211 Folglich gelten die Feststellungen und Erwägungen im Rahmen der Antwort auf die erste Frage in den Rechtssachen C-511/18 und C-512/18 sowie auf die erste und die zweite Frage in der Rechtssache C-520/18 *mutatis mutandis* auch für Art. 23 der Verordnung 2016/679.

212 Nach alledem ist auf die zweite Frage in der Rechtssache C-512/18 zu antworten, dass die Richtlinie 2000/31 dahin auszulegen ist, dass sie im Bereich des Schutzes der Vertraulichkeit der Kommunikation sowie des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten im Rahmen der Dienste der Informationsgesellschaft nicht anwendbar ist; dieser Schutz ist entweder durch die Richtlinie 2002/58 oder durch die Verordnung 2016/679 geregelt. Art. 23 Abs. 1 der Verordnung 2016/679 ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen, dass er einer nationalen Regelung entgegensteht, mit der den Anbietern eines öffentlichen Online-Zugangs zu Kommunikationsdiensten und den Betreibern von Hosting-Diensten eine allgemeine und unterschiedslose Vorratsspeicherung insbesondere von personenbezogenen Daten im Zusammenhang mit diesen Diensten auferlegt wird.

Zur dritten Frage in der Rechtssache C-520/18

213 Mit der dritten Frage in der Rechtssache C-520/18 möchte das vorlegende Gericht wissen, ob ein nationales Gericht eine Bestimmung seines nationalen Rechts anwenden

darf, aufgrund deren es, wenn es im Einklang mit seinem nationalen Recht eine nationale Rechtsvorschrift, mit der den Betreibern elektronischer Kommunikationsdienste u.a. zur Verfolgung der Ziele des Schutzes der nationalen Sicherheit und der Bekämpfung der Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird, wegen ihrer Unvereinbarkeit mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta für rechtswidrig erklärt, zu einer Beschränkung der zeitlichen Wirkungen dieser Erklärung befugt ist.

214 Der Grundsatz des Vorrangs des Unionsrechts besagt, dass das Unionsrecht dem Recht der Mitgliedstaaten vorgeht. Dieser Grundsatz verpflichtet daher alle mitgliedstaatlichen Stellen, den verschiedenen unionsrechtlichen Vorschriften volle Wirksamkeit zu verschaffen, wobei das Recht der Mitgliedstaaten die diesen verschiedenen Vorschriften zuerkannte Wirkung in ihrem Hoheitsgebiet nicht beeinträchtigen darf (Urt. v. 16.7.1964, Costa, 6/64, EU:C:1964:66, S. 1270 und 1271, sowie Urt. v. 19.11.2019, A. K. u.a. [Unabhängigkeit der Disziplinarkammer des Obersten Gerichts], C-585/18, C-624/18 und C-625/18, EU:C:2019:982, Rn. 157 und 158 sowie die dort angeführte Rechtsprechung).

215 Nach dem Grundsatz des Vorrangs des Unionsrechts ist ein nationales Gericht, das im Rahmen seiner Zuständigkeit die Bestimmungen des Unionsrechts anzuwenden hat und eine nationale Regelung nicht im Einklang mit den Anforderungen des Unionsrechts auslegen kann, verpflichtet, für die volle Wirksamkeit dieser Bestimmungen Sorge zu tragen, indem es erforderlichenfalls jede – auch spätere – entgegenstehende Bestimmung des nationalen Rechts aus eigener Entscheidungsbefugnis unangewendet lässt, ohne dass es ihre vorherige Beseitigung auf gesetzgeberischem Weg oder durch irgendein anderes verfassungsrechtliches Verfahren beantragen oder abwarten müsste (Urt. v. 22.6.2010, Melki und Abdeli, C-188/10 und C-189/10, EU:C:2010:363, Rn. 43 und die dort angeführte Rechtsprechung, vom 24.6.2019, Popławski, C-573/17, EU:C:2019:530, Rn. 58, und vom 19.11.2019, A. K. u.a. [Unabhängigkeit der Disziplinarkammer des Obersten Gerichts], C-585/18, C-624/18 und C-625/18, EU:C:2019:982, Rn. 160).

216 Nur der *Gerichtshof* kann in Ausnahmefällen und aus zwingenden Erwägungen der Rechtssicherheit eine vorübergehende Aussetzung der Verdrängungswirkung herbeiführen, die eine unionsrechtliche Vorschrift gegenüber mit ihr unvereinbarem nationalem Recht ausübt. Eine solche zeitliche Beschränkung der Wirkungen einer Auslegung des Unionsrechts durch den *Gerichtshof* kann nur in dem Urteil vorgenommen werden, in dem über die begehrte Auslegung entschieden wird (vgl. in diesem Sinne Urteile vom 23.10.2012, Nelson u.a., C-581/10 und C-629/10, EU:C:2012:657, Rn. 89 und 91, vom 23.4.2020, Herst, C-401/18, EU:C:2020:295, Rn. 56 und 57, sowie vom 25.6.2020, A u.a. [Windkraftanlagen in Aalter und Nevele], C-24/19, EU:C:2020:503, Rn. 84 und die dort angeführte Rechtsprechung).

217 Der Vorrang und die einheitliche Anwendung des Unionsrechts würden beeinträchtigt, wenn nationale Gerichte befugt wären, nationalen Bestimmungen, sei es auch nur vorübergehend, Vorrang vor dem Unionsrecht einzuräumen, gegen das sie verstoßen (vgl. in diesem Sinne Urt. v. 29.7.2019, Inter-Environnement Wallonie und Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, Rn. 177 und die dort angeführte Rechtsprechung).

218 Der *Gerichtshof* hat jedoch in einer Rechtssache, in der es um die Rechtmäßigkeit von Maßnahmen ging, die unter Verstoß gegen die durch das Unionsrecht auferlegte Pflicht zur Durchführung einer vorherigen Prüfung der Umweltverträglichkeit eines Projekts und seiner Verträglichkeit mit einem geschützten Gebiet ergangen waren, entschieden, dass ein nationales Gericht, wenn das innerstaatliche Recht es gestattet, die Wirkungen solcher Maßnahmen ausnahmsweise aufrechterhalten kann, sofern dies durch zwingende Erwägungen gerechtfertigt ist, die im Zusammenhang mit der Notwendigkeit stehen, die tatsächliche und schwerwiegende Gefahr einer Unterbrechung der Stromversorgung im betreffenden Mitgliedstaat abzuwenden, der nicht mit anderen Mitteln und Alternativen, insbesondere im Rahmen des Binnenmarkts, entgegengetreten werden kann. Ihre Aufrechterhaltung darf aber nur für den Zeitraum gelten, der absolut notwendig ist, um die Rechtswidrigkeit zu beseitigen (vgl. in diesem Sinne Urt. v. 29.7.2019, Inter- Environnement Wallonie und Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, Rn. 175, 176, 179 und 181).

219 Im Gegensatz zu dem Versäumnis, einer prozeduralen Pflicht wie der vorherigen Prüfung der Auswirkungen eines Projekts im speziellen Bereich des Umweltschutzes nachzukommen, kann ein Verstoß gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta aber nicht durch ein Verfahren wie das in der vorstehenden Randnummer erwähnte geheilt werden. Würden die Wirkungen nationaler Rechtsvorschriften wie der im Ausgangsverfahren in Rede stehenden aufrechterhalten, würde dies nämlich bedeuten, dass durch die betreffenden Rechtsvorschriften den Betreibern elektronischer Kommunikationsdienste weiterhin Verpflichtungen auferlegt würden, die gegen das Unionsrecht verstoßen und mit schwerwiegenden Eingriffen in die Grundrechte der Personen verbunden sind, deren Daten gespeichert wurden.

220 Das vorlegende Gericht darf somit eine Bestimmung seines nationalen Rechts nicht anwenden, die es ermächtigt, die ihm nach nationalem Recht obliegende Feststellung der Rechtswidrigkeit der im Ausgangsverfahren in Rede stehenden nationalen Rechtsvorschriften in ihren zeitlichen Wirkungen zu beschränken.

221 VZ, WY und XX machen in ihren beim *Gerichtshof* eingereichten Erklärungen geltend, die dritte Frage werfe implizit, aber zwangsläufig die Frage auf, ob das Unionsrecht dem entgegenstehe, dass im Rahmen eines Strafverfahrens Informationen und Beweise verwertet würden, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs-

und Standortdaten erlangt worden seien.

222 Insoweit ist, um dem vorlegenden Gericht eine sachgerechte Antwort zu geben, 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 solche unionsrechtswidrige Vorratsdatenspeicherung erlangten Informationen und Beweise im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, schwere Straftaten begangen zu haben, festzulegen.

223 Nach ständiger Rechtsprechung ist es 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) (vgl. in diesem Sinne Urt. v. 6.10.2015, Târşia, C-69/14, EU:C:2015:662, Rn. 26 und 27, v. 24.10.2018, XC u.a., C-234/17, EU:C:2018:853, Rn. 21 und 22 sowie die dort angeführte Rechtsprechung, und v. 19.12.2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, Rn. 33).

224 Was den Äquivalenzgrundsatz anbelangt, obliegt es dem nationalen Gericht, das mit einem Strafverfahren aufgrund von Informationen oder Beweisen befasst ist, die unter Verstoß gegen die Anforderungen aus der Richtlinie 2002/58 erlangt wurden, zu prüfen, ob das für dieses Verfahren geltende nationale Recht Vorschriften vorsieht, die in Bezug auf die Zulässigkeit und die Verwertung solcher Informationen und Beweise ungünstiger sind als die Vorschriften für Informationen und Beweise, die unter Verstoß gegen innerstaatliches Recht erlangt wurden.

225 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 rechtswidrig erlangte Informationen und Beweise einer Person, die im Verdacht steht, Straftaten begangen zu haben, unangemessene Nachteile zufügen. 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.

226 Nach der Rechtsprechung des *Gerichtshof*s ist das Erfordernis, Informationen und Beweise auszuschließen, die unter Verstoß gegen unionsrechtliche Vorschriften erlangt wurden, 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 (vgl. in diesem Sinne Urt. v. 10.4.2003, Steffensen, C-276/01, EU:C:2003:228, Rn. 76 und 77). 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 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 Verletzung zu verhindern (vgl. in diesem Sinne Urt. v. 10.4.2003, Steffensen, C-276/01, EU:C:2003:228, Rn. 78 und 79).

227 Der Effektivitätsgrundsatz verpflichtet ein nationales Strafgericht somit dazu, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen 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.

228 Nach alledem ist auf die dritte Frage in der Rechtssache C-520/18 zu antworten, dass ein nationales Gericht eine Bestimmung seines nationalen Rechts nicht anwenden darf, die es ermächtigt, die ihm nach nationalem Recht obliegende Feststellung, dass nationale Rechtsvorschriften, mit denen den Betreibern elektronischer Kommunikationsdienste u. a. zur Verfolgung der Ziele des Schutzes der nationalen Sicherheit und der Bekämpfung der Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird, wegen ihrer Unvereinbarkeit mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta rechtswidrig sind, in ihren zeitlichen Wirkungen zu beschränken. Art. 15 Abs. 1 der Richtlinie verpflichtet bei einer Auslegung im Licht des Effektivitätsgrundsatzes ein nationales Strafgericht dazu, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen 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.