Sammlung der Rechtsprechung

URTEIL DES GERICHTSHOFS (Große Kammer)

6. Oktober 2020*

Inhaltsverzeichnis

* Verfahrenssprache: Französisch.

„Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten in der elektronischen Kommunikation – Betreiber elektronischer Kommunikationsdienste – Anbieter von Hosting-Diensten und Internetzugangsanbieter – Allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten – Automatisierte Analyse der Daten – Echtzeit-Zugang zu den Daten – Schutz der nationalen Sicherheit und Bekämpfung des Terrorismus – Bekämpfung der Kriminalität – Richtlinie 2002/58/EG – Geltungsbereich – Art. 1 Abs. 3 und Art. 3 – Vertraulichkeit elektronischer Kommunikation – Schutz – Art. 5 und Art. 15 Abs. 1 – Richtlinie 2000/31/EG – Geltungsbereich – Charta der Grundrechte der Europäischen Union – Art. 4, 6 bis 8 und 11 und Art. 52 Abs. 1 – Art. 4 Abs. 2 EUV“

In den verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18

betreffend Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Conseil d'État (Staatsrat, Frankreich) mit Entscheidungen vom 26. Juli 2018, beim Gerichtshof eingegangen am 3. August 2018 (C-511/18 und C-512/18), und von der Cour constitutionnelle (Verfassungsgerichtshof, Belgien) mit Entscheidung vom 19. Juli 2018, beim Gerichtshof eingegangen am 2. August 2018 (C-520/18), in den Verfahren

La Quadrature du Net (C-511/18 und C-512/18),

French Data Network (C-511/18 und C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 und C-512/18),

Igwan.net (C-511/18)

gegen

Premier ministre (C-511/18 und C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 und C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18),

Beteiligte:

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

und

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

gegen

Conseil des Ministres,

Beteiligte:

Child Focus (C-520/18),

erlässt

DER GERICHTSHOF (Große Kammer)

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

Generalanwalt: M. Campos Sánchez-Bordona,

Kanzler: C. Strömholm, Verwaltungsrätin,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 9. und 10. September 2019,

unter Berücksichtigung der Erklärungen

– von La Quadrature du Net, der Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net und dem Center for Democracy and Technology, vertreten durch A. Fitzjean Ò Cobhthaigh, avocat,

– des French Data Network, vertreten durch Y. Padova, avocat,

– von Privacy International, vertreten durch H. Roy, avocat,

– des Ordre des barreaux francophones et germanophone, vertreten durch E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart und J.-F. Henrotte, avocats,

– der Académie Fiscale ASBL und von UA, vertreten durch J.-P. Riquet,

– der Liga voor Mensenrechten ASBL, vertreten durch J. Vander Velpen, avocat,

– der Ligue des Droits de l'Homme ASBL, vertreten durch R. Jespers und J. Fermon, avocats,

– von VZ, WY und XX, vertreten durch D. Pattyn, avocat,

– von Child Focus, vertreten durch N. Buisseret, K. De Meester und J. Van Cauter, avocats,

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

– der belgischen Regierung, vertreten durch J.-C. Halleux, P. Cottin und C. Pochet als Bevollmächtigte im Beistand von J. Vanpraet, Y. Peeters, S. Depré und E. de Lophem, avocats,

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

– der dänischen Regierung, zunächst vertreten durch J. Nymann-Lindegren, M. Wolff und P. Ngo, dann durch J. Nymann-Lindegren und M. Wolff als Bevollmächtigte,

– der deutschen Regierung, zunächst vertreten durch J. Möller, M. Hellmann, E. Lankenau, R. Kanitz und T. Henze, dann durch J. Möller, M. Hellmann, E. Lankenau und R. Kanitz als Bevollmächtigte,

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

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

– der spanischen Regierung, zunächst vertreten durch L. Aguilera Ruiz und A. Rubio González, dann durch L. Aguilera Ruiz als Bevollmächtigte,

– der zyprischen Regierung, vertreten durch E. Neofytou als Bevollmächtigte,

– der lettischen Regierung, vertreten durch V. Soņeca als Bevollmächtigte,

– der ungarischen Regierung, zunächst vertreten durch M. Z. Fehér und Z. Wagner, dann durch M. Z. Fehér als Bevollmächtigte,

– der niederländischen Regierung, vertreten durch M. K. Bulterman und M. A. M. de Ree als Bevollmächtigte,

– der polnischen Regierung, vertreten durch B. Majczyna, J. Sawicka und M. Pawlicka als Bevollmächtigte,

– der schwedischen Regierung, zunächst vertreten durch H. Shev, H. Eklinder, C. Meyer-Seitz und A. Falk, dann durch H. Shev, H. Eklinder, C. Meyer-Seitz und J. Lundberg als Bevollmächtigte,

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

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

– des Europäischen Datenschutzbeauftragten, vertreten durch T. Zerdick und A. Buchta als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 15. Januar 2020

folgendes

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. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung (im Folgenden: Richtlinie 2002/58) sowie der Art. 12 bis 15 der 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“) (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.

2 Das Ersuchen in der Rechtssache C-511/18 ergeht im Rahmen von Rechtsstreitigkeiten zwischen La Quadrature du Net, dem French Data Network, der Fédération des fournisseurs d’accès à Internet associatifs und Igwan.net einerseits sowie dem Premier ministre (Premierminister, Frankreich), dem Garde des Sceaux, ministre de la Justice (Justizminister, Frankreich), dem Ministre de l’Intérieur (Innenminister, Frankreich) und dem Ministre des Armées (Armeeminister, Frankreich) andererseits wegen der Rechtmäßigkeit des Décret nº 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement (Dekret Nr. 2015-1185 vom 28. September 2015 zur Benennung der spezialisierten Nachrichtendienste, JORF vom 29. September 2015, Text 1 von 97, im Folgenden: Dekret Nr. 2015-1185), des Décret nº 2015-1211, du 1er octobre 2015, relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l’État (Dekret Nr. 2015-1211 vom 1. Oktober 2015 zu Rechtsstreitigkeiten über die Umsetzung der genehmigungspflichtigen nachrichtendienstlichen Techniken und über die Sicherheit des Staates betreffende Dateien, JORF vom 2. Oktober 2015, Text 7 von 108, im Folgenden: Dekret Nr. 2015-1211), des Décret nº 2015-1639, du 11 décembre 2015, relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l’article L. 811-4 du code de la sécurité intérieure (Dekret Nr. 2015-1639 vom 11. Dezember 2015 zur Benennung anderer Dienste als der spezialisierten Nachrichtendienste, die auf die in Titel V des VIII. Buchs des Gesetzbuchs über innere Sicherheit, erlassen in Anwendung von Art. L. 811-4 des Gesetzbuchs über innere Sicherheit, genannten Techniken zurückgreifen dürfen, JORF vom 12. Dezember 2015, Text 28 von 127, im Folgenden: Dekret Nr. 2015-1639), sowie des Décret nº 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement (Dekret Nr. 2016-67 vom 29. Januar 2016 über Techniken zur Gewinnung nachrichtendienstlicher Erkenntnisse, JORF vom 31. Januar 2016, Text 2 von 113, im Folgenden: Dekret Nr. 2016-67).

3 Das Ersuchen in der Rechtssache C-512/18 ergeht im Rahmen von Rechtsstreitigkeiten zwischen dem French Data Network, La Quadrature du Net und der Fédération des fournisseurs d’accès à Internet associatifs einerseits sowie dem Premier ministre (Premierminister, Frankreich) und dem Garde des Sceaux, ministre de la justice (Justizminister, Frankreich), andererseits wegen der Rechtmäßigkeit von Art. R. 10-13 des Code des postes et des communications électroniques (Gesetzbuch für Post und elektronische Kommunikation, im Folgenden: CPCE) und des Décret nº 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d’identifier toute personne ayant contribué à la création d’un contenu mis en ligne (Dekret Nr. 2011-219 vom 25. Februar 2011 über die Speicherung und die Übermittlung von Daten, die die Feststellung der Identität aller Personen ermöglichen, die zur Schaffung von Online-Inhalten beigetragen haben, JORF vom 1. März 2011, Text 32 von 170, im Folgenden: Dekret Nr. 2011-219).

4 Das Ersuchen in der Rechtssache C-520/18 ergeht im Rahmen von Rechtsstreitigkeiten zwischen dem Ordre des barreaux francophones et germanophone, der Académie Fiscale ASBL, UA, der Liga voor Mensenrechten ASBL, der Ligue des Droits de l’Homme ASBL, VZ, WY und XX einerseits sowie dem Conseil des ministres (Ministerrat, Belgien) andererseits wegen der Rechtmäßigkeit der Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (Gesetz über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation, *Moniteur belge* vom 18. Juli 2016, S. 44717, im Folgenden: Gesetz vom 29. Mai 2016).

Rechtlicher Rahmen

Unionsrecht

Richtlinie 95/46

5 Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31) wurde 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 (Datenschutz-Grundverordnung) (ABl. 2016, L 119, S. 1) mit Wirkung vom 25. Mai 2018 aufgehoben. Art. 3 Abs. 2 der Richtlinie 95/46 bestimmte:

„Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,

– die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;

– die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.“

6 Der zu Kapitel III („Rechtsbehelfe, Haftung und Sanktionen“) der Richtlinie 95/46 gehörende Art. 22 lautete:

„Unbeschadet des verwaltungsrechtlichen Beschwerdeverfahrens, das vor Beschreiten des Rechtsweges insbesondere bei der in Artikel 28 genannten Kontrollstelle eingeleitet werden kann, sehen die Mitgliedstaaten vor, dass jede Person bei der Verletzung der Rechte, die ihr durch die für die betreffende Verarbeitung geltenden einzelstaatlichen Rechtsvorschriften garantiert sind, bei Gericht einen Rechtsbehelf einlegen kann.“

Richtlinie 97/66

7 Art. 5 („Vertraulichkeit der Kommunikation“) der Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (ABl. 1997, L 24, S. 1) bestimmt:

„(1) Die Mitgliedstaaten stellen durch innerstaatliche Vorschriften die Vertraulichkeit der mit öffentlichen Telekommunikationsnetzen und öffentlich zugänglichen Telekommunikationsdiensten erfolgenden Kommunikation sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Kommunikationen durch andere Personen als die Benutzer, wenn keine Einwilligung der betroffenen Benutzer vorliegt, es sei denn, diese Personen seien gemäß Artikel 14 Absatz 1 gesetzlich dazu ermächtigt.

(2) Absatz 1 betrifft nicht das rechtlich zulässige Aufzeichnen von Kommunikationen im Rahmen einer rechtmäßigen Geschäftspraxis zum Nachweis einer kommerziellen Transaktion oder einer sonstigen geschäftlichen Kommunikation.“

Richtlinie 2000/31

8 Die Erwägungsgründe 14 und 15 der Richtlinie 2000/31 lauten:

„(14) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ausschließlich Gegenstand der Richtlinie [95/46] und der Richtlinie [97/66], beide Richtlinien sind uneingeschränkt auf die Dienste der Informationsgesellschaft anwendbar. Jene Richtlinien begründen bereits einen gemeinschaftsrechtlichen Rahmen für den Bereich personenbezogener Daten, so dass diese Frage in der vorliegenden Richtlinie nicht geregelt werden muss, um das reibungslose Funktionieren des Binnenmarkts und insbesondere den freien Fluss personenbezogener Daten zwischen den Mitgliedstaaten zu gewährleisten. Die Grundsätze des Schutzes personenbezogener Daten sind bei der Umsetzung und Anwendung dieser Richtlinie uneingeschränkt zu beachten, insbesondere in Bezug auf nicht angeforderte kommerzielle Kommunikation und die Verantwortlichkeit von Vermittlern. Die anonyme Nutzung offener Netze wie des Internets kann diese Richtlinie nicht unterbinden.

(15) Die Vertraulichkeit der Kommunikation ist durch Artikel 5 der Richtlinie [97/66] gewährleistet. Gemäß jener Richtlinie untersagen die Mitgliedstaaten jede Art des Abfangens oder Überwachens dieser Kommunikation durch andere Personen als Sender und Empfänger, es sei denn, diese Personen sind gesetzlich dazu ermächtigt."

9 In Art. 1 der Richtlinie 2000/31 heißt es:

„(1) Diese Richtlinie soll einen Beitrag zum einwandfreien Funktionieren des Binnenmarktes leisten, indem sie den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellt.

(2) Diese Richtlinie sorgt, soweit dies für die Erreichung des in Absatz 1 genannten Ziels erforderlich ist, für eine Angleichung bestimmter für die Dienste der Informationsgesellschaft geltender innerstaatlicher Regelungen, die den Binnenmarkt, die Niederlassung der Diensteanbieter, kommerzielle Kommunikationen, elektronische Verträge, die Verantwortlichkeit von Vermittlern, Verhaltenskodizes, Systeme zur außergerichtlichen Beilegung von Streitigkeiten, Klagemöglichkeiten sowie die Zusammenarbeit zwischen den Mitgliedstaaten betreffen.

(3) Diese Richtlinie ergänzt das auf die Dienste der Informationsgesellschaft anwendbare Gemeinschaftsrecht und lässt dabei das Schutzniveau insbesondere für die öffentliche Gesundheit und den Verbraucherschutz, wie es sich aus Gemeinschaftsrechtsakten und einzelstaatlichen Rechtsvorschriften zu deren Umsetzung ergibt, unberührt, soweit die Freiheit, Dienste der Informationsgesellschaft anzubieten, dadurch nicht eingeschränkt wird.

…

(5) Diese Richtlinie findet keine Anwendung auf

…

b) Fragen betreffend die Dienste der Informationsgesellschaft, die von den Richtlinien [95/46] und [97/66] erfasst werden,

…"

10 Art. 2 der Richtlinie 2000/31 bestimmt:

„Im Sinne dieser Richtlinie bezeichnet der Ausdruck

a) ‚Dienste der Informationsgesellschaft' Dienste im Sinne von Artikel 1 Nummer 2 der Richtlinie 98/34/EG [des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften (ABl. 1998, L 204, S. 37)] in der Fassung der Richtlinie 98/48/EG [des Europäischen Parlaments und des Rates vom 20. Juli 1998 (ABl. 1998, L 217, S. 18)].

…"

11 Art. 15 der Richtlinie 2000/31 sieht vor:

„(1) Die Mitgliedstaaten erlegen Anbietern von Diensten im Sinne der Artikel 12, 13 und 14 keine allgemeine Verpflichtung auf, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

(2) Die Mitgliedstaaten können Anbieter von Diensten der Informationsgesellschaft dazu verpflichten, die zuständigen Behörden unverzüglich über mutmaßliche rechtswidrige Tätigkeiten oder Informationen der Nutzer ihres Dienstes zu unterrichten, oder dazu verpflichten, den zuständigen Behörden auf Verlangen Informationen zu übermitteln, anhand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung geschlossen haben, ermittelt werden können."

Richtlinie 2002/21

12 Der zehnte Erwägungsgrund der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) (ABl. 2002, L 108, S. 33) lautet:

„Die Begriffsbestimmung für ‚Dienste der Informationsgesellschaft' in Artikel 1 der Richtlinie [98/34 in der Fassung der Richtlinie 98/48] umfasst einen weiten Bereich von wirtschaftlichen Tätigkeiten, die online erfolgen. Die meisten dieser Tätigkeiten werden vom Geltungsbereich der vorliegenden Richtlinie nicht erfasst, weil sie nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen. Sprachtelefonie- und E-Mail-Übertragungsdienste werden von dieser Richtlinie erfasst. Dasselbe Unternehmen, beispielsweise ein Internet-Diensteanbieter, kann sowohl elektronische Kommunikationsdienste, wie den Zugang zum Internet, als auch nicht unter diese Richtlinie fallende Dienste, wie die Bereitstellung von Internet-gestützten Inhalten, anbieten."

13 Art. 2 der Richtlinie 2002/21 bestimmt:

„Für die Zwecke dieser Richtlinie gelten folgende Begriffsbestimmungen:

…

c) ‚elektronische Kommunikationsdienste': gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie [98/34], die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen;

…"

Richtlinie 2002/58

14 In den Erwägungsgründen 2, 6, 7, 11, 22, 26 und 30 der Richtlinie 2002/58 heißt es:

„(2) Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die [Charta] anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 [der] Charta niedergelegten Rechte uneingeschränkt geachtet werden.

…

(6) Das Internet revolutioniert die herkömmlichen Marktstrukturen, indem es eine gemeinsame, weltweite Infrastruktur für die Bereitstellung eines breiten Spektrums elektronischer Kommunikationsdienste bietet. Öffentlich zugängliche elektronische Kommunikationsdienste über das Internet eröffnen neue Möglichkeiten für die Nutzer, bilden aber auch neue Risiken in Bezug auf ihre personenbezogenen Daten und ihre Privatsphäre.

(7) Für öffentliche Kommunikationsnetze sollten besondere rechtliche, ordnungspolitische und technische Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und der berechtigten Interessen juristischer Personen erlassen werden, insbesondere im Hinblick auf die zunehmenden Fähigkeiten zur automatischen Speicherung und Verarbeitung personenbezogener Daten über Teilnehmer und Nutzer.

…

(11) Wie die Richtlinie [95/46] gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das [Unionsrecht] fallen. Deshalb hat sie keine Auswirkungen auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten, Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der [am 4. November 1950 in Rom unterzeichneten] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein sowie angemessenen Garantien gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten entsprechen.

…

(22) Mit dem Verbot der Speicherung von Nachrichten und zugehörigen Verkehrsdaten durch andere Personen als die Nutzer oder ohne deren Einwilligung soll die automatische, einstweilige und vorübergehende Speicherung dieser Informationen insoweit nicht untersagt werden, als diese Speicherung einzig und allein zum Zwecke der Durchführung der Übertragung in dem elektronischen Kommunikationsnetz erfolgt und als die Information nicht länger gespeichert wird, als dies für die Übertragung und zum Zwecke der Verkehrsabwicklung erforderlich ist, und die Vertraulichkeit der Nachrichten gewahrt bleibt. …

…

(26) Teilnehmerdaten, die in elektronischen Kommunikationsnetzen zum Verbindungsaufbau und zur Nachrichtenübertragung verarbeitet werden, enthalten Informationen über das Privatleben natürlicher Personen und betreffen ihr Recht auf Achtung ihrer Kommunikationsfreiheit, oder sie betreffen berechtigte Interessen juristischer Personen. Diese Daten dürfen nur für einen begrenzten Zeitraum und nur insoweit gespeichert werden, wie dies für die Erbringung des Dienstes, für die Gebührenabrechnung und für Zusammenschaltungszahlungen erforderlich ist. Jede weitere Verarbeitung solcher Daten … darf nur unter der Bedingung gestattet werden, dass der Teilnehmer dieser Verarbeitung auf der Grundlage genauer, vollständiger Angaben des Betreibers des öffentlich zugänglichen elektronischen Kommunikationsdienstes über die Formen der von ihm beabsichtigten weiteren Verarbeitung und über das Recht des Teilnehmers, seine Einwilligung zu dieser Verarbeitung nicht zu erteilen oder zurückzuziehen, zugestimmt hat. Verkehrsdaten, die für die Vermarktung von Kommunikationsdiensten … verwendet wurden, sollten ferner nach der Bereitstellung des Dienstes gelöscht oder anonymisiert werden. …

…

(30) Die Systeme für die Bereitstellung elektronischer Kommunikationsnetze und -dienste sollten so konzipiert werden, dass so wenig personenbezogene Daten wie möglich benötigt werden. …“

15 Art. 1 („Geltungsbereich und Zielsetzung“) der Richtlinie 2002/58 bestimmt:

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

(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie [95/46] im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des [AEU-Vertrags] fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.“

16 Art. 2 („Begriffsbestimmungen“) der Richtlinie 2002/58 sieht vor:

„Sofern nicht anders angegeben, gelten die Begriffsbestimmungen der Richtlinie [95/46] und der Richtlinie [2002/21] auch für diese Richtlinie.

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

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

b) ‚Verkehrsdaten‘ Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

c) ‚Standortdaten' Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben;

d) ‚Nachricht' jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein elektronisches Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

…"

17 Art. 3 („Betroffene Dienste") der Richtlinie 2002/58 lautet:

„Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen."

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

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

…

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

19 Art. 6 („Verkehrsdaten") der Richtlinie 2002/58 bestimmt:

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

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

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

…

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

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

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

21 Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) der Richtlinie 2002/58 bestimmt:

„(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie [95/46] für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des [Unionsrechts] einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.

…

(2) Die Bestimmungen des Kapitels III der Richtlinie [95/46] über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.

…“

Verordnung 2016/679

22 Im zehnten Erwägungsgrund der Verordnung 2016/679 heißt es:

„Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden. …“

23 Art. 2 der Verordnung 2016/679 bestimmt:

„(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,

…

d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

…

(4) Die vorliegende Verordnung lässt die Anwendung der Richtlinie [2000/31] und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt.“

24 Art. 4 der Verordnung 2016/679 sieht vor:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. ‚personenbezogene Daten‘ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person‘) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. ‚Verarbeitung‘ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das

Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

…“

25 Art. 5 der Verordnung 2016/679 bestimmt:

„(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (‚Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz‘);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken (‚Zweckbindung‘);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (‚Datenminimierung‘);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (‚Richtigkeit‘);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden (‚Speicherbegrenzung‘);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‚Integrität und Vertraulichkeit‘);

…“

26 In Art. 6 der Verordnung 2016/679 heißt es:

„(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

…

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

…

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt … sein … Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten [muss] ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

…“

27 Art. 23 der Verordnung 2016/679 sieht vor:

„(1) Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

a) die nationale Sicherheit;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;

f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind;

i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

j) die Durchsetzung zivilrechtlicher Ansprüche.

(2) Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf

a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,

b) die Kategorien personenbezogener Daten,

c) den Umfang der vorgenommenen Beschränkungen,

d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung,

e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,

f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,

g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und

h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.“

28 Art. 79 Abs. 1 der Verordnung 2016/679 sieht vor:

„Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.“

29 Art. 94 der Verordnung 2016/679 lautet:

„(1) Die Richtlinie [95/46] wird mit Wirkung vom 25. Mai 2018 aufgehoben.

(2) Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie [95/46] eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss.“

30 Art. 95 der Verordnung 2016/679 lautet:

„Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie [2002/58] festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.“

Französisches Recht

Gesetzbuch über innere Sicherheit

31 Das VIII. Buch des legislativen Teils des Code de la sécurité intérieure (Gesetzbuch über innere Sicherheit, im Folgenden: CSI) enthält in seinen Art. L. 801-1 bis L. 898-1 Vorschriften über den Nachrichtendienst.

32 Art. 811-3 des CSI bestimmt:

„Allein für die Ausübung ihrer jeweiligen Aufgaben können die spezialisierten Nachrichtendienste auf die in Titel V des vorliegenden Buchs genannten Techniken zurückgreifen, um Nachrichten in Bezug auf die Verteidigung und die Förderung folgender grundlegender Interessen der Nation zu sammeln:

1. nationale Unabhängigkeit, Integrität des Hoheitsgebiets und nationale Verteidigung;

2. wichtige Interessen der Außenpolitik, Erfüllung der europäischen und internationalen Verpflichtungen Frankreichs und Verhütung jeder Form ausländischer Einmischung;

3. wichtige wirtschaftliche, industrielle und wissenschaftliche Interessen Frankreichs;

4. Verhütung des Terrorismus;

5. Verhütung

a) von Beeinträchtigungen des republikanischen Charakters der Institutionen;

b) von Handlungen zur Aufrechterhaltung oder Wiedererrichtung von Gruppierungen, die in Anwendung von Art. L. 212-1 aufgelöst wurden;

c) von kollektiver Gewalt, die geeignet ist, den öffentlichen Frieden schwer zu beeinträchtigen;

6. Verhütung organisierter Kriminalität und Delinquenz;

7. Verhütung der Verbreitung von Massenvernichtungswaffen.“

33 Art. L. 811-4 des CSI lautet:

„In einem nach Anhörung des Staatsrats und nach Stellungnahme der Nationalen Kommission für die Kontrolle nachrichtendienstlicher Techniken zu erlassenden Dekret werden die dem Verteidigungs-, dem Innen- und dem Justizminister sowie den für die Wirtschaft, den Haushalt oder die Zölle zuständigen Ministern unterstellten Dienste neben den spezialisierten Nachrichtendiensten benannt, die ermächtigt werden können, unter den im vorliegenden Buch aufgestellten Voraussetzungen auf die in dessen Titel V genannten Techniken zurückzugreifen. Für jeden Dienst werden nähere Angaben zu den in Art. L. 811-3 aufgeführten Zielen und den Techniken gemacht, die zu der Ermächtigung führen können.“

34 Art. L. 821-1 Abs. 1 des CSI bestimmt:

„Die Umsetzung der in den Kapiteln I bis IV von Titel V des vorliegenden Buchs genannten Techniken zur Gewinnung nachrichtendienstlicher Erkenntnisse im Inland bedarf der vorherigen Genehmigung des Premierministers, die nach Stellungnahme der Nationalen Kommission für die Kontrolle nachrichtendienstlicher Techniken erteilt wird.“

35 Art. L. 821-2 des CSI sieht vor:

„Die Genehmigung im Sinne von Art. L. 821-1 wird auf schriftlichen, mit einer Begründung versehenen Antrag des Verteidigungsministers, des Innenministers, des Justizministers oder der für die Wirtschaft, den Haushalt oder die Zölle zuständigen Minister erteilt. Jeder Minister kann diese Zuständigkeit nur an direkte Mitarbeiter delegieren, die der Schweigepflicht im Rahmen der Landesverteidigung unterliegen.

In dem Antrag ist Folgendes anzugeben:

1. die anzuwendende(n) Technik(en);

2. der Dienst, für den er gestellt wird;

3. das oder die verfolgte(n) Ziel(e);

4. der Grund oder die Gründe für die Maßnahmen;

5. die Gültigkeitsdauer der Genehmigung;

6. die betroffenen Personen, Orte oder Fahrzeuge.

Im Rahmen der Anwendung von Nr. 6 können Personen, deren Identität nicht bekannt ist, mit ihrer Kennung oder ihrer Eigenschaft bezeichnet werden, und die Orte oder Fahrzeuge können unter Bezugnahme auf die Personen, die Gegenstand des Antrags sind, bezeichnet werden.

…“

36 Art. L. 821-3 Abs. 1 des CSI lautet:

„Der Antrag wird dem Vorsitzenden oder, hilfsweise, einem der in den Nrn. 2 und 3 von Art. L. 831-1 aufgeführten Mitglieder der Nationalen Kommission für die Kontrolle nachrichtendienstlicher Techniken zur Stellungnahme gegenüber dem Premierminister innerhalb von 24 Stunden übermittelt. Wird der Antrag von der Kommission in beschränkter Zusammensetzung oder im Plenum geprüft, wird der Premierminister davon unverzüglich unterrichtet, und die Stellungnahme wird innerhalb von 72 Stunden abgegeben.“

37 Art. L. 821-4 des CSI bestimmt:

„Die Genehmigung zur Umsetzung der in den Kapiteln I bis IV von Titel V des vorliegenden Buchs genannten nachrichtendienstlichen Techniken wird vom Premierminister für höchstens vier Monate erteilt. … Die Genehmigung enthält die in den Nrn. 1 bis 6 von Art. L. 821-2 vorgesehenen Begründungen und Angaben. Jede Genehmigung kann unter den im vorliegenden Kapitel vorgesehenen Voraussetzungen erneut erteilt werden.

Wird die Genehmigung erteilt, nachdem die Nationale Kommission für die Kontrolle nachrichtendienstlicher Techniken eine ablehnende Stellungnahme abgegeben hat, wird in der Genehmigung angegeben, aus welchen Gründen der Stellungnahme nicht gefolgt wurde.

…“

38 Der zu Kapitel III dieses Titels gehörende Art. L. 833-4 des CSI bestimmt:

„Die Kommission prüft von sich aus oder aufgrund einer Beschwerde einer Person, die sicherstellen möchte, dass ihr gegenüber keine nachrichtendienstlichen Techniken in rechtswidriger Weise angewandt werden, die angeführte(n) Technik(en), um zu ermitteln, ob sie unter Beachtung des vorliegenden Buchs umgesetzt wurden oder werden. Sie teilt dem Beschwerdeführer mit, dass die erforderlichen Prüfungen vorgenommen wurden, ohne ihre Umsetzung zu bestätigen oder zu verneinen."

39 Art. L. 841-1 Abs. 1 und 2 des CSI lautet:

„Vorbehaltlich der besonderen Bestimmungen in Art. L. 854-9 des vorliegenden Gesetzbuchs ist der Staatsrat befugt, unter den in Kapitel III*bis* von Titel VII des VIII. Buchs des Verwaltungsgerichtsgesetzes vorgesehenen Voraussetzungen über Anträge auf Umsetzung der in Titel V des vorliegenden Buchs genannten nachrichtendienstlichen Techniken zu entscheiden.

Er kann befasst werden von

1. jeder Person, die sicherstellen möchte, dass ihr gegenüber keine nachrichtendienstlichen Techniken in rechtswidriger Weise angewandt werden, und die nachweist, dass zuvor das in Art. L. 833-4 vorgesehene Verfahren durchgeführt wurde;

2. der Nationalen Kommission für die Kontrolle nachrichtendienstlicher Techniken unter den in Art. L. 833-8 vorgesehenen Voraussetzungen."

40 Kapitel I („Behördlicher Zugang zu Verbindungsdaten") von Titel V („Genehmigungspflichtige Techniken zur Gewinnung nachrichtendienstlicher Erkenntnisse") des VIII. Buchs des legislativen Teils des CSI enthält dessen Art. L. 851-1 bis L. 851-7.

41 Art. L. 851-1 des CSI bestimmt:

„Unter den in Kapitel I von Titel II des vorliegenden Buchs vorgesehenen Voraussetzungen kann gestattet werden, bei den Betreibern elektronischer Kommunikationsdienste und den in Art. L. 34-1 des [CPCE] genannten Personen sowie den in den Nrn. 1 und 2 des Abschnitts I von Art. 6 der Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [Gesetz Nr. 2004-575 vom 21. Juni 2004 für das Vertrauen in die digitale Wirtschaft (JORF vom 22. Juni 2004, S. 11168)] genannten Personen die von ihren Netzen oder elektronischen Kommunikationsdiensten verarbeiteten oder gespeicherten Informationen oder Dokumente zu sammeln, einschließlich technischer Daten in Bezug auf die Ermittlung von Teilnehmer- oder Verbindungsnummern elektronischer Kommunikationsdienste, die Erfassung der Teilnehmer- oder Verbindungsnummern einer bestimmten Person, die Standorte der verwendeten Endgeräte sowie die Kommunikationen eines Teilnehmers, bestehend in der Liste der Nummern ein- und ausgehender Anrufe, der Dauer und des Datums der Kommunikationen.

Abweichend von Art. L. 821-2 werden die schriftlichen und mit einer Begründung versehenen Anträge, die technische Daten in Bezug auf die Ermittlung von Teilnehmer- oder Verbindungsnummern elektronischer Kommunikationsdienste oder die Erfassung aller Teilnehmer- oder Verbindungsnummern einer bestimmten Person betreffen, von den individuell bezeichneten und ermächtigten Bediensteten der in den Art. L. 811-2 und L. 811-4 genannten Nachrichtendienste unmittelbar der Nationalen Kommission für die Kontrolle nachrichtendienstlicher Techniken übermittelt. Die Kommission gibt ihre Stellungnahme unter den in Art. L. 821-3 vorgesehenen Voraussetzungen ab.

Eine Dienststelle des Premierministers wird mit der Sammlung der Informationen oder Dokumente bei den in Abs. 1 des vorliegenden Artikels genannten Betreibern und Personen betraut. Die Nationale Kommission für die Kontrolle nachrichtendienstlicher Techniken verfügt über einen permanenten, umfassenden, direkten und unverzüglichen Zugang zu den gesammelten Informationen oder Dokumenten.

Die Modalitäten für die Anwendung des vorliegenden Artikels werden in einem nach Anhörung des Staatsrats und nach Stellungnahme der Nationalen Kommission für Informatik und Freiheiten und der Nationalen Kommission für die Kontrolle nachrichtendienstlicher Techniken zu erlassenden Dekret festgelegt."

42 In Art. L. 851-2 des CSI heißt es:

„I. – Unter den in Kapitel I von Titel II des vorliegenden Buchs vorgesehenen Voraussetzungen und allein zur Verhütung des Terrorismus kann individuell gestattet werden, in den Netzen der Betreiber und der in Art. L. 851-1 genannten Personen die in diesem Artikel genannten Informationen oder Dokumente über eine Person, von der zuvor festgestellt wurde, dass sie verdächtigt wird, in Verbindung mit einer Bedrohung zu stehen, in Echtzeit zu sammeln. 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.

I*bis*. – Die Höchstzahl der gleichzeitig in Kraft befindlichen, in Anwendung des vorliegenden Artikels erteilten Genehmigungen wird vom Premierminister nach Stellungnahme der Nationalen Kommission für die Kontrolle nachrichtendienstlicher Techniken festgelegt. Die Entscheidung, mit der dieses Kontingent festgelegt und unter den in Abs. 1 von Art. L. 821-2 genannten Ministern aufgeteilt wird, sowie die Zahl der erteilten Überwachungsanordnungen werden der Kommission mitgeteilt.

…"

43 Art. L. 851-3 des CSI sieht vor:

„I. – Unter den in Kapitel I von Titel II des vorliegenden Buchs vorgesehenen Voraussetzungen und allein zur Verhütung des Terrorismus kann den Betreibern und den in Art. L. 851-1 genannten Personen auferlegt werden, in ihren Netzen automatisierte Verarbeitungen vorzunehmen, die dazu dienen, anhand in der Genehmigung angegebener Parameter Verbindungen aufzuspüren, die auf eine terroristische Bedrohung hinweisen können.

Bei diesen automatisierten Verarbeitungen werden ausschließlich die in Art. L. 851-1 genannten Informationen oder Dokumente verwendet, ohne andere Daten zu erheben als die, die den für sie geltenden Parametern entsprechen, und ohne die Identifizierung der Personen zu ermöglichen, auf die sich die Informationen oder Dokumente beziehen.

Unter Beachtung des Grundsatzes der Verhältnismäßigkeit werden in der Genehmigung des Premierministers die technischen Vorgaben für die Vornahme dieser Verarbeitungen festgelegt.

II. – Die Nationale Kommission für die Kontrolle nachrichtendienstlicher Techniken gibt eine Stellungnahme zum Antrag auf Genehmigung automatisierter Verarbeitungen und zu den herangezogenen Detektionsparametern ab. Sie verfügt über einen permanenten, umfassenden und direkten Zugang zu diesen Verarbeitungen sowie zu den gesammelten Informationen und Daten. Sie wird über jede Modifizierung der Verarbeitungen und Parameter unterrichtet und kann Empfehlungen abgeben.

Die erste Genehmigung der in Abschnitt I des vorliegenden Artikels vorgesehenen Vornahme automatisierter Verarbeitungen wird für zwei Monate erteilt. Sie kann im Rahmen der in Kapitel I von Titel II des vorliegenden Buchs vorgesehenen zeitlichen Vorgaben verlängert werden. Der Antrag auf Verlängerung muss eine Aufstellung der Zahl der im Rahmen der automatisierten Verarbeitung gemeldeten Identifikatoren und eine Analyse der Relevanz dieser Meldungen enthalten.

III. – Für die inhaltlichen Maßnahmen zur Vornahme solcher Verarbeitungen durch die Betreiber und die in Art. L. 851-1 genannten Personen gelten die in Art. L. 871-6 vorgesehenen Voraussetzungen.

IV. – Werden bei den in Abschnitt I des vorliegenden Artikels genannten Verarbeitungen Daten aufgespürt, die auf das Vorliegen einer Bedrohung mit terroristischem Charakter hindeuten, kann der Premierminister oder eine der von ihm benannten Personen nach Stellungnahme der Nationalen Kommission für die Kontrolle nachrichtendienstlicher Techniken, die unter den in Kapitel I von Titel II des vorliegenden Buchs vorgesehenen Voraussetzungen abgegeben wird, die Identifizierung des oder der Betroffenen und die Erhebung der damit verbundenen Daten gestatten. Diese Daten werden innerhalb von sechzig Tagen nach ihrer Erhebung ausgewertet und nach Ablauf dieser Frist vernichtet, es sei denn, dass schwerwiegende Gesichtspunkte das Vorliegen einer mit einem oder mehreren der Betroffenen zusammenhängenden terroristischen Bedrohung bestätigen.

…“

44 Art. L. 851-4 des CSI lautet:

„Unter den in Kapitel I von Titel II des vorliegenden Buchs vorgesehenen Voraussetzungen können die technischen Daten über die Standorte der verwendeten Endgeräte im Sinne von Art. L. 851-1 auf Antrag im Netz erhoben und von den Betreibern in Echtzeit einer Dienststelle des Premierministers übermittelt werden.“

45 Der zum verwaltungsrechtlichen Teil des CSI gehörende Art. R. 851-5 sieht vor:

„I. – Bei den in Art. L. 851-1 genannten Informationen und Dokumenten handelt es sich, unter Ausschluss des Inhalts des Schriftwechsels oder der konsultierten Informationen, um

1. die in den Art. R. 10-13 und R. 10-14 des [CPCE] und in Art. 1 des Dekrets [Nr. 2011-219] aufgeführten;

2. die technischen Daten neben den in Nr. 1 genannten,

a) die es gestatten, die Standorte der Endgeräte zu ermitteln;

b) die den Zugang der Endgeräte zu den Netzen oder zu öffentlichen Online-Kommunikationsdiensten betreffen;

c) die die Durchleitung der elektronischen Kommunikation durch die Netze betreffen;

d) die die Identifizierung und die Authentifizierung eines Nutzers, einer Verbindung, eines Netzes oder eines öffentlichen Online-Kommunikationsdienstes betreffen;

e) die die Merkmale der Endgeräte und die Konfigurationsdaten ihrer Software betreffen.

II. – Nur die in Abschnitt I Nr. 1 genannten Informationen und Dokumente dürfen in Anwendung von Art. L. 851-1 gesammelt werden. Sie werden zeitversetzt gesammelt.

Die in Abschnitt I Nr. 2 aufgeführten Informationen dürfen nur in Anwendung der Art. L. 851-2 und L. 851-3, unter den Voraussetzungen und in den Grenzen, die in diesen Artikeln vorgesehen sind, und unbeschadet der Anwendung von Art. R. 851-9 gesammelt werden."

CPCE

46 Art. L. 34-1 des CPCE bestimmt:

„I. – Der vorliegende Artikel gilt für die Verarbeitung personenbezogener Daten im Rahmen des öffentlichen Angebots elektronischer Kommunikationsdienste; er gilt insbesondere für Netze, die Instrumente zur Sammlung von Daten und zur Identifizierung unterstützen.

II. – Die Betreiber elektronischer Kommunikationsdienste und insbesondere die Personen, deren Tätigkeit darin besteht, einen Zugang zu öffentlichen Online-Kommunikationsdiensten anzubieten, löschen oder anonymisieren alle Verkehrsdaten, vorbehaltlich der Bestimmungen in den Abschnitten III, IV, V und VI.

Personen, die der Öffentlichkeit elektronische Kommunikationsdienste anbieten, führen unter Beachtung der Bestimmungen des vorstehenden Absatzes interne Verfahren ein, die es gestatten, den Ersuchen der zuständigen Behörden nachzukommen.

Personen, die im Rahmen einer haupt- oder nebenberuflichen Tätigkeit der Öffentlichkeit eine Verbindung anbieten, die über einen Netzzugang eine Online-Kommunikation ermöglicht, müssen, auch wenn ihr Angebot kostenlos ist, die nach dem vorliegenden Artikel für die Betreiber elektronischer Kommunikationsdienste geltenden Bestimmungen beachten.

III. – Für die Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten oder eines Verstoßes gegen die in Art. L. 336-3 des Code de la propriété intellectuelle [Gesetzbuch über geistiges Eigentum] aufgestellte Verpflichtung oder für die Zwecke der Verhinderung von Beeinträchtigungen der Systeme zur automatisierten Verarbeitung von Daten, mit deren Regelung und Ahndung sich die Art. 323-1 bis 323-3-1 des Code pénal [Strafgesetzbuch] befassen, und allein deshalb, um, soweit erforderlich, die Verfügbarmachung der Justizbehörde oder der in Art. L. 331-12 des Gesetzbuchs über geistiges Eigentum genannten Hohen Behörde oder der in Art. L. 2321-1 des Code de la défense [Verteidigungsgesetzbuch] genannten Nationalen Behörde für die Sicherheit der Informationssysteme zu ermöglichen, können die Maßnahmen zur Löschung oder Anonymisierung bestimmter Kategorien technischer Daten für höchstens ein Jahr aufgeschoben werden. In einem nach Anhörung des Staatsrats und nach Stellungnahme der Nationalen Kommission für Informatik und Freiheiten zu erlassenden Dekret werden innerhalb der in Abschnitt VI festgelegten Grenzen diese Kategorien von Daten und die Dauer ihrer Speicherung, nach Maßgabe der Tätigkeit der Betreiber und der Art der Kommunikationen, sowie die Modalitäten des etwaigen Ausgleichs der ermittelbaren und spezifischen Mehrkosten für die von den Betreibern insoweit auf Ersuchen des Staates erbrachten Leistungen bestimmt.

…

VI. – Die Daten, die unter den in den Abschnitten III, IV und V festgelegten Voraussetzungen gespeichert und verarbeitet wurden, beziehen sich ausschließlich auf die Identifizierung der Nutzer der von den Betreibern angebotenen Dienste, die technischen Merkmale der von ihnen ermöglichten Kommunikationen und den Standort der Endgeräte.

Sie dürfen sich auf keinen Fall auf den Inhalt der ausgetauschten Nachrichten oder auf die Informationen beziehen, die, in welcher Form auch immer, im Rahmen dieser Kommunikationen abgerufen wurden.

Diese Daten werden unter Beachtung der Bestimmungen der Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Gesetz Nr. 78-17 vom 6. Januar 1978 über Informatik, Dateien und Freiheiten] gespeichert und verarbeitet.

Die Betreiber ergreifen alle Maßnahmen, um eine Verwendung dieser Daten zu anderen als den im vorliegenden Artikel vorgesehenen Zwecken zu verhindern."

47 Art. R. 10-13 des CPCE lautet:

„I. – In Anwendung von Abschnitt III des Art. L. 34-1 speichern die Betreiber elektronischer Kommunikationsdienste für die Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten

a) Informationen, die es erlauben, den Nutzer zu identifizieren;

b) Daten über die verwendeten Kommunikationsendgeräte;

c) die technischen Merkmale sowie Datum, Uhrzeit und Dauer jeder Kommunikation;

d) Daten über beantragte oder in Anspruch genommene Zusatzleistungen und deren Anbieter;

e) Daten, die es erlauben, die Identität des oder der Adressaten der Nachrichtenübermittlung festzustellen.

II. – Im Fernmeldebereich speichert der Betreiber die in Abschnitt II genannten Daten sowie die Daten, die es ermöglichen, die Herkunft und den Standort der Kommunikation zu bestimmen.

III. – Die im vorliegenden Artikel genannten Daten werden für die Dauer eines Jahres ab dem Tag der Aufzeichnung gespeichert.

IV. – Die ermittelbaren und spezifischen Mehrkosten der Betreiber, denen von den Justizbehörden auferlegt wird, die zu den im vorliegenden Artikel genannten Kategorien gehörenden Daten zu liefern, werden gemäß den in Art. R. 213-1 des Strafgesetzbuchs vorgesehenen Modalitäten ausgeglichen."

48 Art. R. 10-14 des CPCE sieht vor:

„I. – In Anwendung von Abschnitt IV des Art. L. 34-1 sind die Betreiber elektronischer Kommunikationsdienste befugt, für die Bedürfnisse ihrer Rechnungsstellung und des Zahlungsverkehrs die technischen Daten zu speichern, die es ermöglichen, den Nutzer zu identifizieren, sowie die in den Buchst. b, c und d von Abschnitt I des Art. R. 10-13 genannten Daten.

II. – Im Fernmeldebereich können die Betreiber neben den in Abschnitt I genannten Daten technische Daten in Bezug auf den Standort der Kommunikation und die Identifizierung des oder der Adressaten der Kommunikation sowie Daten zur Ermöglichung der Rechnungsstellung speichern.

III. – Die in den Abschnitten I und II des vorliegenden Artikels genannten Daten dürfen nur gespeichert werden, wenn sie für die Rechnungsstellung und die Bezahlung der geleisteten Dienste erforderlich sind. Ihre Speicherung muss sich auf die zu diesem Zweck zwingend erforderliche Zeit beschränken und darf ein Jahr nicht überschreiten.

IV. – Für die Sicherheit der Netze und Einrichtungen können die Betreiber folgende Daten für höchstens drei Monate speichern:

a) Daten, die es erlauben, die Identität des Urhebers der Kommunikation festzustellen;

b) die technischen Merkmale sowie Datum, Uhrzeit und Dauer jeder Kommunikation;

c) technische Daten, die es erlauben, die Identität des oder der Adressaten der Kommunikation festzustellen;

d) Daten über beantragte oder in Anspruch genommene Zusatzleistungen und deren Anbieter."

Gesetz Nr. 2004-575 vom 21. Juni 2004 für das Vertrauen in die digitale Wirtschaft

49 Art. 6 der Loi n° 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (Gesetz Nr. 2004-575 vom 21. Juni 2004 für das Vertrauen in die digitale Wirtschaft, JORF vom 22. Juni 2004, S. 11168, im Folgenden: LCEN) sieht vor:

„I. – (1) Personen, deren Tätigkeit darin besteht, der Öffentlichkeit einen Online-Zugang zu Kommunikationsdiensten anzubieten, informieren ihre Teilnehmer darüber, dass es technische Mittel gibt, die es gestatten, den Zugang zu bestimmten Diensten zu beschränken oder sie auszuwählen, und bieten ihnen mindestens eines dieser Mittel an.

…

(2) Natürliche oder juristische Personen, die, sei es auch kostenlos, zur Bereitstellung für die Öffentlichkeit durch öffentliche Online-Kommunikationsdienste die Speicherung der von den Adressaten dieser Dienste gelieferten Signale, Schriftstücke, Bilder, Töne oder Botschaften jeder Art gewährleisten, können für Tätigkeiten oder für Informationen, die auf Verlangen eines Adressaten dieser Dienste gespeichert wurden, nicht zivilrechtlich verantwortlich gemacht werden, wenn sie nicht tatsächlich Kenntnis von ihrem rechtswidrigen Charakter oder von Tatsachen und Umständen, aus denen sich dieser Charakter ergab, hatten oder wenn sie, sobald sie davon Kenntnis erlangten, unverzüglich tätig wurden, um diese Daten zu entfernen oder den Zugang zu ihnen unmöglich zu machen.

…

II. – Die in den Abs. 1 und 2 von Abschnitt I genannten Personen erheben und speichern die Daten in einer Weise, die die Identifizierung jeder Person ermöglicht, die zur Schaffung des Inhalts oder eines der Inhalte der von ihnen erbrachten Dienste beigetragen hat.

Sie liefern den Personen, die einen öffentlichen Online-Kommunikationsdienst betreiben, die technischen Mittel, die es ihnen ermöglichen, die in Abschnitt III vorgesehenen Voraussetzungen für die Identifizierung zu erfüllen.

Die Justizbehörde kann von den in den Abs. 1 und 2 von Abschnitt I genannten Leistungserbringern die Übermittlung der in Abs. 1 des vorliegenden Abschnitts genannten Daten verlangen.

Für die Verarbeitung dieser Daten gelten die Bestimmungen der Art. 226-17, 226-21 und 226-22 des Strafgesetzbuchs.

In einem nach Anhörung des Staatsrats und nach Stellungnahme der Nationalen Kommission für Informatik und Freiheiten zu erlassenden Dekret werden die in Abs. 1 genannten Daten festgelegt sowie die Dauer und die Modalitäten ihrer Speicherung bestimmt.

…"

Dekret Nr. 2011-219

50 Kapitel I des auf der Grundlage von Art. 6 Abschnitt II, letzter Absatz, der LCEN ergangenen Dekrets Nr. 2011-219 enthält dessen Art. 1 bis 4.

51 Art. 1 des Dekrets Nr. 2011-219 bestimmt:

„Die in Abschnitt II von Art 6 der [LCEN] genannten und nach dieser Bestimmung zu speichernden Daten sind:

1. für die in Abs. 1 von Abschnitt I dieses Artikels genannten Personen und für jede Verbindung ihrer Teilnehmer

a) die Kennung der Verbindung;

b) die dem Teilnehmer von diesen Personen zugewiesene Kennung;

c) die Kennung des für die Verbindung genutzten Endgeräts, falls sie Zugang dazu haben;

d) Datum und Uhrzeit von Beginn und Ende der Verbindung;

e) die Merkmale der Leitung des Teilnehmers;

2. für die in Abs. 2 von Abschnitt I dieses Artikels genannten Personen und für jeden Vorgang

a) die Kennung der Verbindung, von der die Kommunikation ausging;

b) die dem Inhalt, der Gegenstand des Vorgangs ist, vom Informationssystem zugewiesene Kennung;

c) die Arten der für die Verbindung zum Dienst und für die Übertragung der Inhalte verwendeten Protokolle;

d) die Art des Vorgangs;

e) Datum und Uhrzeit des Vorgangs;

f) die vom Urheber des Vorgangs benutzte Kennung, falls er sie angegeben hat;

3. für die in den Abs. 1 und 2 von Abschnitt I dieses Artikels genannten Personen folgende beim Abschluss eines Vertrags durch einen Nutzer oder bei der Einrichtung eines Kontos gelieferten Informationen:

a) die Kennung dieser Verbindung zum Zeitpunkt der Einrichtung des Kontos;

b) Name und Vorname bzw. Firma;

c) die verknüpften Postanschriften;

d) die verwendeten Aliasnamen;

e) die verknüpften E-Mail- oder Kontoadressen;

f) die Telefonnummern;

g) das Passwort sowie die Angaben, die seine Überprüfung oder Änderung ermöglichen, in ihrer aktuellen Fassung;

4. für die in den Abs. 1 und 2 von Abschnitt I dieses Artikels genannten Personen, wenn der Abschluss des Vertrags oder die Einrichtung des Kontos kostenpflichtig ist, für jeden Zahlungsvorgang folgende die Zahlung betreffende Informationen:

a) die verwendete Zahlungsart;

b) die Zahlungsreferenz;

c) den Betrag,

d) Datum und Uhrzeit der Transaktion.

Die in den Nrn. 3 und 4 genannten Daten sind nur zu speichern, soweit die Personen sie üblicherweise sammeln."

52 Art. 2 des Dekrets lautet:

„Der Beitrag zur Schaffung von Inhalten umfasst folgende Vorgänge:

a) die ursprüngliche Schaffung von Inhalten;

b) Änderungen der Inhalte und mit den Inhalten verknüpfter Daten;

c) die Löschung von Inhalten."

53 Art. 3 des Dekrets sieht vor:

„Die in Art. 1 genannten Daten werden für die Dauer eines Jahres gespeichert, und zwar

a) hinsichtlich der in den Nrn. 1 und 2 genannten Daten für jeden Vorgang, der im Sinne von Art. 2 zur Schaffung eines Inhalts beiträgt, ab dem Tag der Schaffung der Inhalte;

b) hinsichtlich der in Nr. 3 genannten Daten ab dem Tag der Auflösung des Vertrags oder der Schließung des Kontos;

c) hinsichtlich der in Nr. 4 genannten Daten für jede Rechnung und jeden Zahlungsvorgang ab dem Tag der Erstellung der Rechnung oder des Zahlungsvorgangs."

Belgisches Recht

54 Mit dem Gesetz vom 29. Mai 2016 wurden u. a. die Loi du 13 juin 2005 relative aux communications électroniques (Gesetz vom 13. Juni 2005 über die elektronische Kommunikation, *Moniteur belge* vom 20. Juni 2005, S. 28070, im Folgenden: Gesetz vom 13. Juni 2005), der Code d'instruction criminelle (Strafprozessgesetzbuch) und die Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste, *Moniteur belge* vom 18. Dezember 1998, S. 40312, im Folgenden: Gesetz vom 30. November 1998) abgeändert.

55 Art. 126 des Gesetzes vom 13. Juni 2005 in der Fassung des Gesetzes vom 29. Mai 2016 bestimmt:

„§ 1 – Unbeschadet des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten speichern öffentliche Anbieter von Telefon-, Internetzugangs-, Internet-E-Mail- und Internet-Telefonie-Diensten, Betreiber öffentlicher elektronischer Kommunikationsnetze und Betreiber eines der beiden Dienste auf Vorrat in § 3 erwähnte Daten, die bei der Bereitstellung der betreffenden Kommunikationsdienste von ihnen erzeugt oder verarbeitet werden.

Vorliegender Artikel bezieht sich nicht auf den Inhalt der Kommunikationen.

Die Verpflichtung zur Vorratsspeicherung der in § 3 erwähnten Daten gilt ebenfalls für erfolglose Anrufversuche, sofern diese Daten bei der Bereitstellung der betreffenden Kommunikationsdienste:

1. von Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste beziehungsweise eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, wenn es sich um Telefoniedaten handelt, oder

2. von diesen Anbietern protokolliert werden, wenn es sich um Internetdaten handelt.

§ 2 – Nur folgende Behörden dürfen auf einfaches Verlangen von den in § 1 Absatz 1 erwähnten Anbietern und Betreibern Daten erhalten, die aufgrund des vorliegenden Artikels für folgende Zwecke und gemäß den nachstehend aufgezählten Bedingungen auf Vorrat gespeichert werden:

1. Gerichtsbehörden im Hinblick auf Ermittlung, Untersuchung und Verfolgung von Verstößen, zur Ausführung von Maßnahmen, die in den Artikeln 46*bis* und 88*bis* des Strafprozessgesetzbuchs erwähnt sind, und unter den durch diese Artikel festgelegten Bedingungen,

2. Nachrichten- und Sicherheitsdienste zur Erfüllung von nachrichtendienstlichen Aufträgen unter Einsatz der in den Artikeln 16/2, 18/7 und 18/8 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Methoden zur Datensammlung und gemäß den in vorliegendem Gesetz festgelegten Bedingungen,

3. Gerichtspolizeioffiziere des [Belgischen Instituts für Post- und Fernmeldewesen] im Hinblick auf Ermittlung, Untersuchung und Verfolgung von Verstößen gegen die Artikel 114, 124 und vorliegenden Artikel,

4. Hilfsdienste, die Hilfe vor Ort anbieten, wenn sie nach einem Notruf vom betreffenden Anbieter oder Betreiber mit Hilfe der in Artikel 107 § 2 Absatz 3 erwähnten Datenbank nicht die Identifizierungsdaten des Anrufers oder unvollständige oder fehlerhafte Daten erhalten. Nur die Identifizierungsdaten des Anrufers dürfen binnen einer Frist von maximal 24 Stunden nach dem Anruf beantragt werden,

5. Gerichtspolizeioffiziere der Vermisstenzelle der Föderalen Polizei im Rahmen ihres Auftrags zur Hilfeleistung für Personen in Gefahr, Suche nach vermissten Personen, deren Verschwinden als Besorgnis erregend angesehen wird, und wenn es schwerwiegende Vermutungen oder Indizien dafür gibt, dass die körperliche Unversehrtheit der vermissten Person unmittelbar in Gefahr ist. Nur die in § 3 Absatz 1 und 2 erwähnten Daten über die vermisste Person, die während 48 Stunden vor dem Antrag auf Erhalt der Daten auf Vorrat gespeichert wurden, dürfen beim betreffenden Betreiber oder Anbieter über einen vom König bestimmten Polizeidienst beantragt werden,

6. der Ombudsdienst für Telekommunikation im Hinblick auf die Identifizierung von Personen, die gemäß den Bedingungen wie in Artikel 43*bis* § 3 Nr. 7 des Gesetzes vom 21. März 1991 zur Umstrukturierung bestimmter öffentlicher Wirtschaftsunternehmen erwähnt böswillig ein elektronisches Kommunikationsnetz beziehungsweise einen elektronischen Kommunikationsdienst genutzt haben. Nur die Identifizierungsdaten dürfen beantragt werden.

Die in § 1 Absatz 1 erwähnten Anbieter und Betreiber sorgen dafür, dass in § 3 erwähnte Daten von Belgien aus unbeschränkt zugänglich sind und dass diese Daten und alle anderen notwendigen Informationen zu diesen Daten unverzüglich und nur den in vorliegendem Paragraphen erwähnten Behörden übermittelt werden können.

Unbeschadet anderer Gesetzesbestimmungen dürfen in § 1 Absatz 1 erwähnte Anbieter und Betreiber die aufgrund von § 3 auf Vorrat gespeicherten Daten nicht für andere Zwecke nutzen.

§ 3 – Daten zur Identifizierung von Nutzer oder Teilnehmer und Kommunikationsmittel, in den Absätzen 2 und 3 spezifisch vorgesehene Daten ausgenommen, werden zwölf Monate ab dem Datum, an dem eine Kommunikation über den benutzten Dienst zum letzten Mal möglich ist, auf Vorrat gespeichert.

Daten in Bezug auf Zugang und Verbindung der Endeinrichtung zu Netzwerk und Dienst und in Bezug auf den Standort dieser Ausrüstung, einschließlich des Netzabschlusspunktes, werden zwölf Monate ab dem Datum der Kommunikation auf Vorrat gespeichert.

Kommunikationsdaten mit Ausnahme des Inhalts, einschließlich ihres Ursprungs und ihrer Bestimmung, werden zwölf Monate ab dem Datum der Kommunikation auf Vorrat gespeichert.

Der König legt auf Vorschlag des Ministers der Justiz und des [für die Angelegenheiten in Bezug auf elektronische Kommunikation zuständigen] Ministers und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts durch einen im Ministerrat beratenen Erlass die nach Art der in Absatz 1 bis 3 erwähnten Kategorien auf Vorrat zu speichernden Daten und die Anforderungen, die diese Daten erfüllen müssen, fest.

…“

Ausgangsverfahren und Vorlagefragen

Rechtssache C-511/18

56 Mit Klageschriften, die am 30. November 2015 und am 16. März 2016 eingingen und im Ausgangsverfahren verbunden wurden, haben La Quadrature du Net, das French Data Network und die Fédération des fournisseurs d’accès à Internet associatifs sowie Igwan.net beim Conseil d’État (Staatsrat, Frankreich) Klagen auf Nichtigerklärung der Dekrete Nrn. 2015-1185, 2015-1211, 2015-1639 und 2016-67 erhoben. Zur Begründung haben sie u. a. vorgetragen, die Dekrete verstießen gegen die französische Verfassung, die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) sowie die Richtlinien 2000/31 und 2002/58 im Licht der Art. 7, 8 und 47 der Charta.

57 Speziell in Bezug auf den Klagegrund des Verstoßes gegen die Richtlinie 2000/31 führt das vorlegende Gericht aus, die Bestimmungen von Art. L. 851-3 des CSI verpflichteten die Betreiber elektronischer Kommunikationsdienste und technische Dienstleister, „in ihren Netzen automatisierte Verarbeitungen vorzunehmen, die dazu dienen, anhand in der Genehmigung angegebener Parameter Verbindungen aufzuspüren, die auf eine terroristische Bedrohung hinweisen können“. Diese Technik ziele darauf ab,

für begrenzte Zeit unter allen von diesen Betreibern und Dienstleistern verarbeiteten Verbindungsdaten allein diejenigen zu sammeln, die einen Zusammenhang mit einer solchen schweren Zuwiderhandlung aufweisen könnten. Unter diesen Umständen verstießen die genannten Bestimmungen, mit denen keine allgemeine Pflicht zu aktiver Überwachung auferlegt werde, nicht gegen Art. 15 der Richtlinie 2000/31.

58 In Bezug auf den Klagegrund des Verstoßes gegen die Richtlinie 2002/58 führt das vorlegende Gericht aus, wie insbesondere aus den Bestimmungen dieser Richtlinie und aus dem Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, im Folgenden: Urteil Tele2, EU:C:2016:970), hervorgehe, fielen nationale Bestimmungen, die den Betreibern elektronischer Kommunikationsdienste Pflichten wie die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten ihrer Nutzer und Teilnehmer zu den in Art. 15 Abs. 1 der Richtlinie genannten Zwecken, zu denen der Schutz der nationalen Sicherheit, der Landesverteidigung und der öffentlichen Sicherheit gehöre, auferlegten, in den Geltungsbereich der Richtlinie, soweit diese Regelungen die Tätigkeit der genannten Betreiber regelten. Das Gleiche gelte für Regelungen des Zugangs nationaler Behörden zu diesen Daten und ihrer Nutzung.

59 Folglich fielen in den Geltungsbereich der Richtlinie 2002/58 sowohl die Speicherungspflicht, die sich aus Art. L. 851-1 des CSI ergebe, als auch der in den Art. L. 851-1, L. 851-2 und L. 851-4 des CSI vorgesehene behördliche Zugang zu den Daten, einschließlich des Echtzeit-Zugangs. Das Gleiche gelte für die Bestimmungen von Art. L. 851-3 des CSI, die den Betreibern zwar keine allgemeine Speicherungspflicht auferlegten, sie aber verpflichteten, in ihren Netzen automatisierte Verarbeitungen vorzunehmen, die dazu dienten, Verbindungen aufzuspüren, die auf eine terroristische Bedrohung hinweisen könnten.

60 Die in den Nichtigkeitsklagen angeführten Bestimmungen des CSI über Techniken zur Sammlung von Informationen, die unmittelbar vom Staat umgesetzt würden, ohne die Tätigkeiten der Betreiber elektronischer Kommunikationsdienste zu regeln und ihnen spezielle Pflichten aufzuerlegen, fielen dagegen nicht in den Geltungsbereich der Richtlinie 2002/58. In ihnen könne keine Umsetzung des Unionsrechts gesehen werden, so dass nicht mit Erfolg gerügt werden könne, dass sie gegen diese Richtlinie verstießen.

61 Die Entscheidung über die Streitigkeiten betreffend die Rechtmäßigkeit der Dekrete Nrn. 2015-1185, 2015-1211, 2015-1639 und 2016-67 im Hinblick auf die Richtlinie 2002/58, soweit sie zur Umsetzung der Art. L. 851-1 bis L. 851-4 des CSI ergangen seien, hänge somit von drei Fragen nach der Auslegung des Unionsrechts ab.

62 Erstens stelle sich hinsichtlich der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 die Frage, ob eine allgemeine und unterschiedslose Speicherungspflicht, wie sie den Betreibern elektronischer Kommunikationsdienste auf der Grundlage der Art. L. 851-1 und R. 851-5 des CSI auferlegt werde, insbesondere angesichts der Garantien und Kontrollen, die für den behördlichen Zugang zu den Verbindungsdaten und ihre Nutzung vorgesehen seien, als ein durch das Recht auf Sicherheit, das durch Art. 6 der Charta gewährleistet werde, und durch die Anforderungen der nationalen Sicherheit, für die nach Art. 4 EUV allein die Mitgliedstaaten verantwortlich seien, gerechtfertigter Eingriff anzusehen sei.

63 Was zweitens die übrigen Pflichten anbelange, die den Betreibern elektronischer Kommunikationsdienste auferlegt werden könnten, gestatteten die Bestimmungen von Art. L. 851-2 des CSI allein für die Zwecke der Verhütung des Terrorismus die in dessen Art. L. 851-1 vorgesehene Sammlung von Informationen oder Dokumenten bei den gleichen Personen. Ihre Sammlung, die nur eine oder mehrere Personen betreffe, von denen zuvor festgestellt worden sei, dass sie Verbindungen zu einer terroristischen Bedrohung haben könnten, erfolge in Echtzeit. Das Gleiche gelte für die Bestimmungen von Art. L. 851-4 des CSI, die es den Betreibern gestatteten, allein die technischen Daten zum Standort der Endgeräte in Echtzeit zu übermitteln. Diese Techniken regelten mit

unterschiedlicher Zielsetzung und mittels verschiedener Modalitäten den behördlichen Zugang zu den gemäß dem CPCE und der LCEN gespeicherten Daten in Echtzeit, ohne die betreffenden Betreiber mit einem zusätzlichen, über das, was zur Fakturierung und Erbringung ihrer Dienste erforderlich sei, hinausgehenden Speicherungserfordernis zu belasten. Desgleichen implizierten auch die Bestimmungen von Art. L. 851-3 des CSI, die die Diensteanbieter verpflichteten, in ihren Netzen eine automatisierte Analyse der Verbindungen vorzunehmen, keine allgemeine und unterschiedslose Speicherung.

64 Zum einen böten aber sowohl die allgemeine und unterschiedslose Speicherung als auch der Echtzeit-Zugang zu den Verbindungsdaten in einem durch ernste und anhaltende Bedrohungen der nationalen Sicherheit, insbesondere aufgrund der Gefahr des Terrorismus, gekennzeichneten Kontext einen einzigartigen operationellen Nutzen. Die allgemeine und unterschiedslose Speicherung verschaffe den Nachrichtendiensten nämlich einen Zugang zu den die Kommunikationen betreffenden Daten, bevor die Gründe ermittelt worden seien, auf denen die Annahme beruhe, dass die betreffende Person eine Bedrohung für die öffentliche Sicherheit, die Landesverteidigung oder die Sicherheit des Staates darstelle. Außerdem erlaube der Echtzeit-Zugang zu den Verbindungsdaten es, das Verhalten von Personen, die eine unmittelbare Bedrohung für die öffentliche Ordnung darstellen könnten, mit hoher Reaktivität zu verfolgen.

65 Zum anderen erlaube es die in Art. L. 851-3 des CSI vorgesehene Technik, anhand von gerade zu diesem Zweck aufgestellten Kriterien Personen aufzuspüren, deren Verhalten angesichts ihrer Kommunikationsweise auf eine terroristische Bedrohung hindeuten könne.

66 Drittens stelle sich hinsichtlich des Zugangs der zuständigen Behörden zu den gespeicherten Daten die Frage, ob die Richtlinie 2002/58 im Licht der Charta dahin auszulegen sei, dass sie die Rechtmäßigkeit der Verfahren zur Erhebung von Verbindungsdaten stets davon abhängig mache, dass die Betroffenen unterrichtet würden, wenn ihre Unterrichtung die Ermittlungen der zuständigen Behörden nicht mehr beeinträchtigen könne, oder ob solche Verfahren in Anbetracht aller anderen im nationalen Recht vorgesehenen Verfahrensgarantien als rechtmäßig angesehen werden könnten, wenn diese Garantien die Wirksamkeit des Rechts auf Einlegung eines Rechtsbehelfs gewährleisteten.

67 In Bezug auf diese anderen Verfahrensgarantien sei insbesondere darauf hinzuweisen, dass jede Person, die prüfen lassen wolle, ob eine nachrichtendienstliche Technik ihr gegenüber in unzulässiger Weise umgesetzt werde, einen speziellen Spruchkörper des Conseil d'État (Staatsrat) anrufen könne, der anhand der ihm außerhalb des kontradiktorischen Verfahrens mitgeteilten Gesichtspunkte darüber zu entscheiden habe, ob im Fall des Klägers eine solche Technik zum Einsatz gekommen sei und ob dies im Einklang mit dem VIII. Buch des CSI geschehen sei. Die diesem Spruchkörper bei der Bearbeitung der Klagen zustehenden Befugnisse gewährleisteten die Wirksamkeit der von ihm ausgeübten gerichtlichen Kontrolle. So könne er bei der Bearbeitung der Klagen von Amts wegen alle von ihm festgestellten Rechtsfehler aufgreifen und der Verwaltung aufgeben, alle sachgerechten Maßnahmen zu ergreifen, um den festgestellten Rechtsfehlern abzuhelfen. Außerdem habe die Nationale Kommission für die Kontrolle nachrichtendienstlicher Techniken zu prüfen, ob die nachrichtendienstlichen Techniken zur Sammlung von Informationen im Inland im Einklang mit den Anforderungen des CSI umgesetzt würden. Somit stelle der Umstand, dass die im Ausgangsverfahren in Rede stehenden Rechtsvorschriften nicht vorsähen, dass die Betroffenen von den gegen sie gerichteten Überwachungsmaßnahmen unterrichtet würden, für sich genommen keine übermäßige Beeinträchtigung des Rechts auf Achtung des Privatlebens dar.

68 Unter diesen Umständen hat der Conseil d'État (Staatsrat) das Verfahren ausgesetzt und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorgelegt:

1. Ist die den Betreibern auf der Grundlage der permissiven Bestimmungen in Art. 15 Abs. 1 der Richtlinie 2002/58 auferlegte Pflicht zur allgemeinen und unterschiedslosen Speicherung in einem durch ernste und anhaltende Bedrohungen der nationalen Sicherheit, insbesondere durch die

Gefahr des Terrorismus, gekennzeichneten Kontext als ein Eingriff anzusehen, der durch das in Art. 6 der Charta garantierte Recht auf Sicherheit und die Erfordernisse der nach Art. 4 EUV in die alleinige Verantwortung der Mitgliedstaaten fallenden nationalen Sicherheit gerechtfertigt ist?

2. Ist die Richtlinie 2002/58 im Licht der Charta dahin auszulegen, dass sie gesetzgeberische Maßnahmen wie die Maßnahmen zur Erhebung von Verkehrs- und Standortdaten bestimmter Personen in Echtzeit gestattet, die zwar die Rechte und Pflichten der Betreiber elektronischer Kommunikationsdienste berühren, ihnen aber keine spezielle Pflicht zur Speicherung ihrer Daten auferlegen?

3. Ist die Richtlinie 2002/58 im Licht der Charta dahin auszulegen, dass sie die Rechtmäßigkeit der Verfahren zur Erhebung von Verbindungsdaten stets von dem Erfordernis abhängig macht, dass die betroffenen Personen unterrichtet werden, wenn ihre Unterrichtung die behördlichen Ermittlungen nicht mehr beeinträchtigen kann, oder können solche Verfahren in Anbetracht aller übrigen bestehenden Verfahrensgarantien als rechtmäßig angesehen werden, wenn diese Garantien die Wirksamkeit des Rechts auf Einlegung eines Rechtsbehelfs gewährleisten?

Rechtssache C-512/18

69 Mit Klageschrift, die am 1. September 2015 einging, haben das French Data Network, La Quadrature du Net und die Fédération des fournisseurs d'accès à Internet associatifs beim Conseil d'État (Staatsrat) Klage auf Nichtigerklärung der aus dem Schweigen des Premierministers auf ihren Antrag, Art. R. 10-13 des CPCE und das Dekret Nr. 2011-219 u. a. wegen Verstoßes gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 der Charta aufzuheben, resultierenden stillschweigenden ablehnenden Entscheidung für nichtig zu erklären. Privacy International und das Center for Democracy and Technology sind im Ausgangsverfahren als Streithelfer zugelassen worden.

70 Zu Art. R. 10-13 des CPCE und der darin vorgesehenen Pflicht zur allgemeinen und unterschiedslosen Speicherung von Kommunikationsdaten führt das vorlegende Gericht mit ähnlichen Erwägungen wie in der Rechtssache C-511/18 aus, eine solche Speicherung verschaffe der Justizbehörde Zugriff auf Daten über Kommunikationen, die ein Einzelner getätigt habe, bevor er in den Verdacht geraten sei, eine Straftat begangen zu haben; sie biete daher einen einzigartigen Nutzen für die Ermittlung, Feststellung und Verfolgung von Straftaten.

71 Zum Dekret Nr. 2011-219 stellt das vorlegende Gericht fest, Abschnitt II von Art. 6 der LCEN, der eine Pflicht zur Erhebung und Speicherung allein der die Schaffung von Inhalten betreffenden Daten vorsehe, falle nicht in den Geltungsbereich der Richtlinie 2002/58, der sich nach deren Art. 3 Abs. 1 auf die Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union beschränke, sondern in den Geltungsbereich der Richtlinie 2000/31.

72 Wie sich aus Art. 15 Abs. 1 und 2 der Richtlinie 2000/31 ergebe, enthalte sie aber kein grundsätzliches Verbot, die Schaffung von Inhalten betreffende Daten zu speichern, von dem nur ausnahmsweise abgewichen werden könnte. Somit stelle sich die Frage, ob die Art. 12, 14 und 15 dieser Richtlinie im Licht der Art. 6 bis 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen seien, dass sie es einem Mitgliedstaat gestatteten, eine nationale Regelung wie Art. 6 Abschnitt II der LCEN einzuführen, mit der die Betroffenen verpflichtet würden, Daten so zu speichern, dass jede Person, die zur Schaffung des Inhalts oder eines der Inhalte der von ihnen erbrachten Dienste beigetragen habe, identifiziert werden könne, damit die Justizbehörde gegebenenfalls ihre Übermittlung verlangen könne, um für die Beachtung der Vorschriften über die zivil- oder strafrechtliche Haftung zu sorgen.

73 Unter diesen Umständen hat der Conseil d'État (Staatsrat) das Verfahren ausgesetzt und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorgelegt:

1. Ist die den Betreibern auf der Grundlage der permissiven Bestimmungen in Art. 15 Abs. 1 der Richtlinie 2002/58 auferlegte Pflicht zur allgemeinen und unterschiedslosen Speicherung, insbesondere angesichts der Garantien und Kontrollen, die anschließend in Bezug auf die Erhebung und Nutzung dieser Verbindungsdaten bestehen, als ein Eingriff anzusehen, der durch das in Art. 6 der Charta garantierte Recht auf Sicherheit und die Erfordernisse der nach Art. 4 EUV in die alleinige Verantwortung der Mitgliedstaaten fallenden nationalen Sicherheit gerechtfertigt ist?

2. Sind die Bestimmungen der Richtlinie 2000/31 im Licht der Art. 6, 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen, dass sie es einem Staat gestatten, eine nationale Regelung einzuführen, mit der Personen, deren Tätigkeit darin besteht, der Öffentlichkeit einen Online-Zugang zu Kommunikationsdiensten anzubieten, und natürliche oder juristische Personen, die, sei es auch kostenlos, zur Bereitstellung für die Öffentlichkeit durch öffentliche Online-Kommunikationsdienste die Speicherung der von den Adressaten dieser Dienste gelieferten Signale, Schriftstücke, Bilder, Töne oder Botschaften jeder Art gewährleisten, verpflichtet werden, Daten so zu speichern, dass jede Person, die zur Schaffung des Inhalts oder eines der Inhalte der von ihnen erbrachten Dienste beigetragen hat, identifiziert werden kann, damit die Justizbehörde gegebenenfalls ihre Übermittlung verlangen kann, um für die Beachtung der Vorschriften über die zivil- oder strafrechtliche Haftung zu sorgen?

Rechtssache C-520/18

74 Mit Klageschriften, die am 10., 16., 17. und 18. Januar 2017 eingingen und im Ausgangsverfahren verbunden wurden, haben der Ordre des barreaux francophones et germanophone, die Académie Fiscale ASBL, UA, die Liga voor Mensenrechten ASBL und die Ligue des Droits de l'Homme ASBL sowie VZ, WY und XX bei der Cour constitutionnelle (Verfassungsgerichtshof, Belgien) Klagen auf Nichtigerklärung des Gesetzes vom 29. Mai 2016 wegen Verstoßes gegen die Art. 10 und 11 der belgischen Verfassung in Verbindung mit den Art. 5, 6 bis 11, 14, 15, 17 und 18 der EMRK, den Art. 7, 8, 11 und 47 sowie von Art. 52 Abs. 1 der Charta, Art. 17 des von der Generalversammlung der Vereinten Nationen am 16. Dezember 1966 angenommenen und am 23. März 1976 in Kraft getretenen Internationalen Pakts über bürgerliche und politische Rechte, der allgemeinen Grundsätze der Rechtssicherheit, der Verhältnismäßigkeit und der informationellen Selbstbestimmung sowie von Art. 5 Abs. 4 EUV erhoben.

75 Zur Stützung ihrer Klagen machen die Kläger des Ausgangsverfahrens im Wesentlichen geltend, das Gesetz vom 29. Mai 2016 sei vor allem deshalb rechtswidrig, weil es die Grenzen des absolut Notwendigen überschreite und keine hinreichenden Schutzgarantien vorsehe. Insbesondere genügten weder seine Bestimmungen über die Speicherung von Daten noch die Bestimmungen über den Zugang der Behörden zu den gespeicherten Daten den Anforderungen, die sich aus dem Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, im Folgenden: Urteil Digital Rights, EU:C:2014:238), und dem Urteil vom 21. Dezember 2016, Tele2 (C-203/15 und C-698/15, EU:C:2016:970), ergäben. Mit diesen Bestimmungen sei nämlich die Gefahr verbunden, dass Persönlichkeitsprofile erstellt würden, was zu Missbräuchen durch die zuständigen Behörden führen könnte, und sie sähen auch kein angemessenes Niveau der Sicherung und des Schutzes der gespeicherten Daten vor. Schließlich erstrecke sich das Gesetz auf Personen, die einem Berufsgeheimnis unterworfen seien, sowie auf Personen, die zur Vertraulichkeit verpflichtet seien, und betreffe sensible personenbezogene Kommunikationsdaten, ohne spezielle Garantien zum Schutz dieser Daten zu enthalten.

76 Die von den Anbietern von Telefon-, Internetzugangs-, Internet-E-Mail- und Internet-Telefonie-Diensten sowie den Betreibern öffentlicher elektronischer Kommunikationsnetze nach dem Gesetz vom 29. Mai 2016 zu speichernden Daten stimmten mit den in der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58 (ABl. 2006, L 105, S. 54) aufgeführten Daten überein, ohne dass eine Unterscheidung hinsichtlich der Betroffenen oder anhand des verfolgten Ziels vorgesehen sei. Der Gesetzgeber verfolge mit dem Gesetz vom 29. Mai 2016 nicht nur das Ziel der Bekämpfung des Terrorismus und der Kinderpornografie, sondern wolle die gespeicherten Daten auch in einer Vielzahl von Situationen im Rahmen der Strafverfolgung nutzen. Wie aus der Begründung des Gesetzes hervorgehe, habe der nationale Gesetzgeber es im Licht des verfolgten Ziels für unmöglich erachtet, eine gezielte und differenzierte Speicherungspflicht einzuführen, und sich dafür entschieden, die allgemeine und unterschiedslose Speicherungspflicht sowohl auf der Ebene der gespeicherten Daten als auch auf der Ebene des Zugangs zu ihnen mit strikten Garantien zu versehen, um den Eingriff in das Recht auf Achtung des Privatlebens auf ein Minimum zu begrenzen.

77 Art. 126 Abs. 2 Nrn. 1 und 2 des Gesetzes vom 13. Juni 2005 in der Fassung des Gesetzes vom 29. Mai 2016 sehe vor, unter welchen Voraussetzungen die Gerichtsbehörden bzw. die Nachrichten- und Sicherheitsdienste Zugang zu den gespeicherten Daten erhalten könnten, so dass die Prüfung der Rechtmäßigkeit dieses Gesetzes anhand der Anforderungen des Unionsrechts ausgesetzt werden müsse, bis der Gerichtshof über zwei bei ihm anhängige Vorabentscheidungsersuchen entschieden habe, die einen solchen Zugang beträfen.

78 Schließlich solle das Gesetz vom 29. Mai 2016 eine effektive strafrechtliche Untersuchung und eine wirksame Bestrafung des sexuellen Missbrauchs von Minderjährigen sowie die Identifizierung des Täters einer solchen Straftat ermöglichen, auch wenn von elektronischen Kommunikationsmitteln Gebrauch gemacht werde. Im gerichtlichen Verfahren sei die Aufmerksamkeit insoweit auf die positiven Verpflichtungen in den Art. 3 und 8 der EMRK gelenkt worden. Diese Verpflichtungen könnten sich ferner aus den entsprechenden Bestimmungen der Charta ergeben, was Folgen für die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 haben könne.

79 Unter diesen Umständen hat der Verfassungsgerichtshof beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Ist Art. 15 Abs. 1 der Richtlinie 2002/58 in Verbindung mit dem Recht auf Sicherheit, das durch Art. 6 der Charta garantiert wird, und dem Recht auf Schutz der personenbezogenen Daten, wie es durch Art. 7, Art. 8 und Art. 52 Abs. 1 der Charta garantiert wird, dahin auszulegen, dass er einer nationalen Regelung wie der des Ausgangsverfahrens entgegensteht, die eine allgemeine Verpflichtung für Betreiber und Anbieter von elektronischen Kommunikationsdiensten vorsieht, die Verkehrs- und Standortdaten im Sinne der Richtlinie 2002/58 auf Vorrat zu speichern, die von ihnen im Rahmen der Bereitstellung dieser Dienste erzeugt oder verarbeitet werden, wenn diese nationale Regelung nicht nur das Ziel der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, sondern auch die Sicherstellung der nationalen Sicherheit, der Landesverteidigung, der öffentlichen Sicherheit, die Ermittlung, Feststellung und Verfolgung von anderen Taten als denen der schweren Kriminalität oder die Verhütung eines untersagten Gebrauchs von elektronischen Kommunikationssystemen oder die Erreichung eines sonstigen Ziels verfolgt, das in Art. 23 Abs. 1 der Verordnung 2016/679 aufgeführt ist und das zudem den in diesen Rechtsvorschriften für die Vorratsspeicherung von Daten und den Zugang zu diesen genau festgelegten Garantien unterliegt?

2. Ist Art. 15 Abs. 1 der Richtlinie 2002/58 in Verbindung mit den Art. 4, 7, 8, 11 und Art. 52 Abs. 1 der Charta dahin auszulegen, dass er einer nationalen Regelung wie der des Ausgangsverfahrens entgegensteht, die eine allgemeine Verpflichtung für Betreiber und Anbieter von elektronischen Kommunikationsdiensten vorsieht, die Verkehrs- und Standortdaten im Sinne der Richtlinie

2002/58 auf Vorrat zu speichern, die von ihnen im Rahmen der Bereitstellung dieser Dienste erzeugt oder verarbeitet werden, wenn diese nationale Regelung insbesondere den Zweck hat, positive Verpflichtungen zu erfüllen, die der Behörde aufgrund der Art. 4 und [7] der Charta obliegen und die darin bestehen, einen gesetzlichen Rahmen vorzusehen, der eine wirksame strafrechtliche Ermittlung und eine wirksame Ahndung des sexuellen Missbrauchs von Minderjährigen ermöglicht und der eine wirkliche Identifizierung des Täters der Straftat ermöglicht, auch wenn von elektronischen Kommunikationsmitteln Gebrauch gemacht wird?

3. Falls der Verfassungsgerichtshof auf der Grundlage der Antworten auf die erste oder zweite Vorabentscheidungsfrage zu dem Schluss gelangen sollte, dass das angefochtene Gesetz gegen eine oder mehrere der Verpflichtungen verstößt, die sich aus den in diesen Fragen genannten Bestimmungen ergeben, könnte er die Folgen des Gesetzes vom 29. Mai 2016 vorläufig aufrechterhalten, um eine Rechtsunsicherheit zu vermeiden und zu ermöglichen, dass die zuvor gesammelten und auf Vorrat gespeicherten Daten noch für die durch das Gesetz angestrebten Ziele benutzt werden können?

Verfahren vor dem Gerichtshof

80 Mit Beschluss des Präsidenten des Gerichtshofs vom 25. September 2018 sind die Rechtssachen C-511/18 und C-512/18 zu gemeinsamem schriftlichen und mündlichen Verfahren und zu gemeinsamer Entscheidung verbunden worden. Die Rechtssache C-520/18 ist durch Beschluss des Präsidenten des Gerichtshofs vom 9. Juli 2020 mit diesen Rechtssachen zu gemeinsamer Entscheidung verbunden worden.

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.

86 Während sowohl der Conseil d'État (Staatsrat) als auch der Verfassungsgerichtshof von der Prämisse ausgehen, dass die in den Ausgangsverfahren in Rede stehenden nationalen Regelungen für die Speicherung von Verkehrs- und Standortdaten sowie den Zugang der nationalen Behörden zu ihnen zu den in Art. 15 Abs. 1 der Richtlinie 2002/58 vorgesehenen Zwecken wie dem Schutz der nationalen Sicherheit in den Geltungsbereich dieser Richtlinie fallen, sind einige Parteien der Ausgangsverfahren sowie einige Mitgliedstaaten, die beim Gerichtshof schriftliche Erklärungen eingereicht haben, insoweit anderer Ansicht, insbesondere in Bezug auf die Auslegung von Art. 1 Abs. 3 der Richtlinie. Daher ist zunächst zu prüfen, ob die genannten Regelungen in den Geltungsbereich der Richtlinie fallen.

Zum Geltungsbereich der Richtlinie 2002/58

87 La Quadrature du Net, die Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International und das Center for Democracy and Technology tragen im Wesentlichen, insoweit gestützt auf die Rechtsprechung des Gerichtshofs zum Geltungsbereich der Richtlinie 2002/58, vor, sowohl die Vorratsspeicherung der Daten als auch der Zugang zu den gespeicherten Daten fielen in

den Geltungsbereich der Richtlinie, unabhängig davon, ob der Zugang in Echtzeit erfolge oder nicht. Da das Ziel des Schutzes der nationalen Sicherheit in Art. 15 Abs. 1 der Richtlinie ausdrücklich erwähnt werde, führe seine Verfolgung nämlich nicht zu ihrer Unanwendbarkeit. Der von den vorlegenden Gerichten angesprochene Art. 4 Abs. 2 EUV ändere daran nichts.

88 Zu den nachrichtendienstlichen Maßnahmen, die von den zuständigen französischen Behörden unmittelbar umgesetzt werden, ohne die Tätigkeit der Betreiber elektronischer Kommunikationsdienste durch die Auferlegung spezifischer Verpflichtungen zu regeln, führt das Center for Democracy and Technology aus, diese Maßnahmen fielen notwendigerweise in den Geltungsbereich der Richtlinie 2002/58 und der Charta, da sie Ausnahmen von dem durch Art. 5 der Richtlinie garantierten Grundsatz der Vertraulichkeit darstellten. Derartige Maßnahmen müssten somit den Anforderungen von Art. 15 Abs. 1 der Richtlinie genügen.

89 Die französische, die tschechische und die estnische Regierung, Irland, die zyprische, die ungarische, die polnische und die schwedische Regierung sowie die Regierung des Vereinigten Königreichs machen hingegen im Wesentlichen geltend, die Richtlinie 2002/58 gelte nicht für nationale Regelungen wie die in den Ausgangsverfahren in Rede stehenden, da sie auf den Schutz der nationalen Sicherheit abzielten. Die zur Aufrechterhaltung der öffentlichen Ordnung sowie zum Schutz der inneren Sicherheit und der Integrität des Hoheitsgebiets dienenden Tätigkeiten der Nachrichtendienste gehörten zu den grundlegenden Funktionen der Mitgliedstaaten und fielen deshalb in ihre alleinige Zuständigkeit, wie insbesondere Art. 4 Abs. 2 Satz 3 EUV zeige.

90 Diese Regierungen sowie Irland verweisen überdies auf Art. 1 Abs. 3 der Richtlinie 2002/58, wonach Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung und die Sicherheit des Staates von ihrem Geltungsbereich ausgeschlossen seien, wie es bereits bei der Richtlinie 95/46 nach deren Art. 3 Abs. 2 erster Gedankenstrich der Fall gewesen sei. Sie stützen sich dabei auf die Auslegung der letztgenannten Bestimmung im Urteil vom 30. Mai 2006, Parlament/Rat und Kommission (C-317/04 und C-318/04, EU:C:2006:346).

91 Hierzu ist festzustellen, dass die Richtlinie 2002/58 nach ihrem Art. 1 Abs. 1 u. a. eine Harmonisierung der Vorschriften der Mitgliedstaaten vorsieht, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation zu gewährleisten.

92 Nach Art. 1 Abs. 3 der Richtlinie 2002/58 sind von ihrem Geltungsbereich die „Tätigkeiten des Staates“ in den dort vorgesehenen Bereichen ausgeschlossen, zu denen die Tätigkeiten des Staates im strafrechtlichen Bereich sowie die Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung und die Sicherheit des Staates einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt, gehören. Die dort beispielhaft aufgeführten Tätigkeiten sind allesamt spezifische Tätigkeiten der Staaten oder staatlicher Stellen, die nichts mit den Tätigkeitsbereichen von Privatpersonen zu tun haben (Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 32 und die dort angeführte Rechtsprechung).

93 Nach Art. 3 der Richtlinie 2002/58 gilt sie für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen (im Folgenden: elektronische Kommunikationsdienste). Folglich ist davon auszugehen, dass diese Richtlinie die Tätigkeiten der Betreiber solcher Dienste regelt (Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 33 und die dort angeführte Rechtsprechung).

94 In diesem Rahmen können die Mitgliedstaaten nach Art. 15 Abs. 1 der Richtlinie 2002/58 unter den dort angegebenen Voraussetzungen „Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken“ (Urteil vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 71).

95 Art. 15 Abs. 1 der Richtlinie 2002/58 setzt nämlich zwangsläufig voraus, dass die dort genannten nationalen Rechtsvorschriften in den Geltungsbereich der Richtlinie fallen, da sie die Mitgliedstaaten zum Erlass solcher Vorschriften ausdrücklich nur dann ermächtigt, wenn die in dieser Bestimmung vorgesehenen Voraussetzungen eingehalten werden. Außerdem regeln diese Rechtsvorschriften – zu den in dieser Bestimmung genannten Zwecken – die Tätigkeit der Betreiber elektronischer Kommunikationsdienste (Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 34 und die dort angeführte Rechtsprechung).

96 Vor allem anhand dieser Erwägungen ist der Gerichtshof zu dem Schluss gelangt, dass Art. 15 Abs. 1 der Richtlinie 2002/58 in Verbindung mit ihrem Art. 3 dahin auszulegen ist, dass in den Geltungsbereich der Richtlinie nicht nur eine Rechtsvorschrift fällt, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, die Verkehrs- und Standortdaten zu speichern, sondern auch eine Rechtsvorschrift, die ihnen vorschreibt, den zuständigen nationalen Behörden Zugang zu diesen Daten zu gewähren. Solche Vorschriften haben nämlich zwangsläufig eine Verarbeitung der betreffenden Daten durch die Betreiber zur Folge und können, da sie die Tätigkeiten dieser Betreiber regeln, den in Art. 1 Abs. 3 der Richtlinie genannten spezifischen Tätigkeiten der Staaten nicht gleichgestellt werden (vgl. in diesem Sinne Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 35 und 37 sowie die dort angeführte Rechtsprechung).

97 Außerdem würde in Anbetracht der Erwägungen in Rn. 95 des vorliegenden Urteils und der Systematik der Richtlinie 2002/58 eine Auslegung, wonach die Rechtsvorschriften, auf die sich ihr Art. 15 Abs. 1 bezieht, von ihrem Geltungsbereich ausgeschlossen sind, weil sich die Zweckbestimmungen, denen solche Rechtsvorschriften entsprechen müssen, im Wesentlichen mit den Zielen decken, die mit den in Art. 1 Abs. 3 der Richtlinie genannten Tätigkeiten verfolgt werden, Art. 15 Abs. 1 jede praktische Wirksamkeit nehmen (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 72 und 73).

98 Der Begriff „Tätigkeiten“ in Art. 1 Abs. 3 der Richtlinie 2002/58 kann daher, wie der Generalanwalt in Nr. 75 seiner Schlussanträge in den verbundenen Rechtssachen La Quadrature du Net u. a. (C-511/18 und C-512/18, EU:C:2020:6) im Wesentlichen ausgeführt hat, nicht so ausgelegt werden, dass er sich auf die Rechtsvorschriften im Sinne von Art. 15 Abs. 1 der Richtlinie erstreckt.

99 Die Bestimmungen von Art. 4 Abs. 2 EUV, auf die die in Rn. 89 des vorliegenden Urteils genannten Regierungen Bezug nehmen, können diese Auslegung nicht in Frage stellen. Denn nach ständiger Rechtsprechung des Gerichtshofs ist es zwar Sache der Mitgliedstaaten, ihre wesentlichen Sicherheitsinteressen festzulegen und die geeigneten Maßnahmen zu ergreifen, um ihre innere und äußere Sicherheit zu gewährleisten, doch kann die bloße Tatsache, dass eine nationale Maßnahme zum Schutz der nationalen Sicherheit getroffen wurde, nicht zur Unanwendbarkeit des Unionsrechts führen und die Mitgliedstaaten von der erforderlichen Beachtung dieses Rechts entbinden (vgl. in diesem Sinne Urteile vom 4. Juni 2013, ZZ, C-300/11, EU:C:2013:363, Rn. 38, vom 20. März 2018, Kommission/Österreich [Staatsdruckerei], C-187/16, EU:C:2018:194, Rn. 75 und 76, sowie vom 2. April 2020, Kommission/Polen, Ungarn und Tschechische Republik [Vorübergehender Umsiedlungsmechanismus für internationalen Schutz beantragende Personen], C-715/17, C-718/17 und C-719/17, EU:C:2020:257, Rn. 143 und 170).

100 Es trifft zu, dass der Gerichtshof im Urteil vom 30. Mai 2006, Parlament/Rat und Kommission (C-317/04 und C-318/04, EU:C:2006:346, Rn. 56 bis 59), entschieden hat, dass die Übermittlung personenbezogener Daten durch Fluggesellschaften an die Behörden eines Drittstaats zur Verhütung

und Bekämpfung des Terrorismus und anderer schwerer Straftaten nach Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 nicht in deren Anwendungsbereich fiel, weil sie in einem von staatlichen Stellen geschaffenen Rahmen stattfand und der öffentlichen Sicherheit diente.

101 Angesichts der Erwägungen in den Rn. 93, 95 und 96 des vorliegenden Urteils ist diese Rechtsprechung jedoch nicht auf die Auslegung von Art. 1 Abs. 3 der Richtlinie 2002/58 übertragbar. Wie der Generalanwalt in den Nrn. 70 bis 72 seiner Schlussanträge in den verbundenen Rechtssachen La Quadrature du Net u. a. (C-511/18 und C-512/18, EU:C:2020:6) im Wesentlichen ausgeführt hat, nahm Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46, auf den sich die genannte Rechtsprechung bezieht, nämlich „Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung [und] die Sicherheit des Staates“ generell vom Anwendungsbereich dieser Richtlinie aus, ohne anhand des Urhebers der betreffenden Verarbeitung von Daten zu unterscheiden. Dagegen erweist sich eine solche Unterscheidung im Rahmen der Auslegung von Art. 1 Abs. 3 der Richtlinie 2002/58 als erforderlich. Wie aus den Rn. 94 bis 97 des vorliegenden Urteils hervorgeht, fallen alle Verarbeitungen personenbezogener Daten durch Betreiber elektronischer Kommunikationsdienste nämlich in ihren Geltungsbereich, einschließlich Verarbeitungen aufgrund von Verpflichtungen, die ihnen von den Behörden auferlegt wurden. Die letztgenannten Verarbeitungen konnten hingegen gegebenenfalls unter die in Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 vorgesehene Ausnahme fallen, da diese Bestimmung weiter gefasst ist und sich auf alle die öffentliche Sicherheit, die Landesverteidigung oder die Sicherheit des Staates betreffenden Verarbeitungen erstreckt, unabhängig von ihrem Urheber.

102 Überdies ist festzustellen, dass die Richtlinie 95/46, um die es in der Rechtssache ging, in der das Urteil vom 30. Mai 2006, Parlament/Rat und Kommission (C-317/04 und C-318/04, EU:C:2006:346), ergangen ist, gemäß Art. 94 Abs. 1 der Verordnung 2016/679 mit Wirkung vom 25. Mai 2018 durch diese aufgehoben und ersetzt wurde. Die Verordnung findet zwar nach ihrem Art. 2 Abs. 2 Buchst. d keine Anwendung auf Verarbeitungen „durch die zuständigen Behörden“ u. a. zum Zweck der Verhütung und Feststellung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Wie aus Art. 23 Abs. 1 Buchst. d und h der Verordnung hervorgeht, fallen aber Verarbeitungen personenbezogener Daten, die zu diesem Zweck von Privatpersonen vorgenommen werden, in ihren Anwendungsbereich. Daraus folgt, dass die vorstehende Auslegung von Art. 1 Abs. 3, Art. 3 und Art. 15 Abs. 1 der Richtlinie 2002/58 im Einklang mit der Abgrenzung des Anwendungsbereichs der Verordnung 2016/679 steht, die diese Richtlinie ergänzt und präzisiert.

103 Wenn die Mitgliedstaaten unmittelbar Maßnahmen umsetzen, mit denen von der Vertraulichkeit elektronischer Kommunikationen abgewichen wird, ohne den Betreibern elektronischer Kommunikationsdienste Verarbeitungspflichten aufzuerlegen, fällt der Schutz der Daten der Betroffenen hingegen nicht unter die Richtlinie 2002/58, sondern allein unter das nationale Recht, vorbehaltlich der Anwendung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. 2016, L 119, S. 89), so dass die fraglichen Maßnahmen insbesondere mit nationalem Recht von Verfassungsrang und den Anforderungen der EMRK im Einklang stehen müssen.

104 Aus den vorstehenden Erwägungen folgt, dass eine nationale Regelung, die wie die in den Ausgangsverfahren in Rede stehenden die Betreiber elektronischer Kommunikationsdienste zum Schutz der nationalen Sicherheit und zur Bekämpfung der Kriminalität zur Vorratsspeicherung von Verkehrs- und Standortdaten verpflichtet, in den Geltungsbereich der Richtlinie 2002/58 fällt.

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 Urteil vom 17. April 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 Einwilligung 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 (Urteil vom 21. Dezember 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 Urteil vom 21. Dezember 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 Satz 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 Urteil vom 2. Oktober 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 Satz 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 Urteile vom 8. April 2014, Digital Rights, C-293/12 und C-594/12, EU:C:2014:238, Rn. 25 und 70, sowie vom 21. Dezember 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 Urteile vom 6. März 2001, Connolly/Kommission, C-274/99 P, EU:C:2001:127, Rn. 39, und vom 21. Dezember 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] vom 26. Juli 2017, EU:C:2017:592, Rn. 124 und 126 sowie die dort angeführte Rechtsprechung; vgl. entsprechend, in Bezug auf Art. 8 der EMRK, EGMR, 30. Januar 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, 16. Februar 2000, Amann gegen Schweiz, CE:ECHR:2000:0216JUD002779895, § 69, sowie 13. Februar 2020, Trjakovski und Chipovski gegen Nordmazedonien, CE:ECHR:2020:0213JUD005320513, § 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. Juli 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 Urteile vom 8. April 2014, Digital Rights, C-293/12 und C-594/12, EU:C:2014:238, Rn. 27, und vom 21. Dezember 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 Urteile vom 8. April 2014, Digital Rights, C-293/12 und C-594/12, EU:C:2014:238, Rn. 28, und vom 21. Dezember 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. Oktober 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 Urteil vom 16. Juli 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 Urteile vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 47, vom 28. Juli 2016, JZ, C-294/16 PPU, EU:C:2016:610, Rn. 48, und vom 19. September 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 Urteile vom 12. Februar 2019, TC, C-492/18 PPU, EU:C:2019:108, Rn. 57, und vom 21. Mai 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, 18. März 2008, Ladent gegen Polen, CE:ECHR:2008:0318JUD001103603, §§ 45 und 46, 29. März 2010, Medvedyev und andere gegen Frankreich, CE:ECHR:2010:0329JUD000339403, §§ 76 und 77, sowie 13. Dezember 2012, El-Masri gegen „The former Yugoslav Republic of Macedonia", CE:ECHR:2012:1213JUD003963009, § 239). Da diese Bestimmung einen Freiheitsentzug 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 Urteil vom 18. Juni 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 Europäische Gerichtshof für Menschenrechte hat nämlich entschieden, dass die den Art. 3 und 8 der EMRK zu entnehmenden positiven Verpflichtungen, denen die Garantien in den Art. 4 und 7 der 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, 28. Oktober 1998, Osman gegen Vereinigtes Königreich, CE:ECHR:1998:1028JUD002345294, §§ 115 und 116, 4. März 2004, M.C. gegen Bulgarien, CE:ECHR:2003:1204JUD003927298, § 151, 24. Juni 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 Satz 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 Urteile vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 56, vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 76, 77 und 86, sowie vom 8. April 2014, Digital Rights, C-293/12 und C-594/12, EU:C:2014:238, Rn. 52; Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 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 Urteil vom 2. Oktober 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 Urteile vom 8. April 2014, Digital Rights, C-293/12 und C-594/12, EU:C:2014:238, Rn. 54 und 55, sowie vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 117; Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 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. Juli 2017, EU:C:2017:592, Rn. 191 und die dort angeführte Rechtsprechung, sowie Urteil vom 3. Oktober 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 Urteile vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 102, und vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 56 und 57; Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 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 Urteil vom 21. Dezember 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 Urteile vom 8. April 2014, Digital Rights, C-293/12 und C-594/12, EU:C:2014:238, Rn. 57 und 58, sowie vom 21. Dezember 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 Urteile vom 8. April 2014, Digital Rights, C-293/12 und C-594/12, EU:C:2014:238, Rn. 59, und vom 21. Dezember 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 Urteil vom 21. Dezember 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 Urteil vom 21. Dezember 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 nicht diskriminierender 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 Urteil vom 21. Dezember 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. c 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 Urteil vom 2. Oktober 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 Satz 1 der Richtlinie 2002/58 genannten Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein können (vgl. in diesem Sinne Urteil vom 2. Oktober 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. November 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 oder verändert 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 Urteil vom 21. Dezember 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. Juli 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. Juli 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 einer 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. Juli 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. Juli 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, 8. Februar 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 Urteil vom 21. Dezember 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 Urteil vom 21. Dezember 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 Urteil vom 21. Dezember 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. Juli 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. Juli 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 unterschiedslose 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 Urteile vom 24. November 2011, Scarlet Extended, C-70/10, EU:C:2011:771, Rn. 40, vom 16. Februar 2012, SABAM, C-360/10, EU:C:2012:85, Rn. 34, vom 15. September 2016, Mc Fadden, C-484/14, EU:C:2016:689, Rn. 55, und vom 7. August 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 Urteil vom 29. Januar 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 Urteil vom 5. Juni 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 Urteil vom 5. Juni 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 Urteil vom 13. Juni 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 Urteil vom 16. Juli 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, Urteil vom 30. Mai 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, Urteil vom 20. Mai 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, Urteil vom 7. November 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 (Urteile vom 15. Juli 1964, Costa, 6/64, EU:C:1964:66, S. 1270 und 1271, sowie vom 19. November 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 (Urteile vom 22. Juni 2010, Melki und Abdeli, C-188/10 und C-189/10, EU:C:2010:363, Rn. 43 und die dort angeführte Rechtsprechung, vom 24. Juni 2019, Popławski, C-573/17, EU:C:2019:530, Rn. 58, und vom 19. November 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. Oktober 2012, Nelson u. a., C-581/10 und C-629/10, EU:C:2012:657, Rn. 89 und 91, vom 23. April 2020, Herst, C-401/18, EU:C:2020:295, Rn. 56 und 57, sowie vom 25. Juni 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 Urteil vom 29. Juli 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 Urteil vom 29. Juli 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 Urteile vom 6. Oktober 2015, Târşia, C-69/14, EU:C:2015:662, Rn. 26 und 27, vom 24. Oktober 2018, XC u. a., C-234/17, EU:C:2018:853, Rn. 21 und 22 sowie die dort angeführte Rechtsprechung, und vom 19. Dezember 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 Gerichtshofs 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 Urteil vom 10. April 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 Urteil vom 10. April 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.

Kosten

229 Für die Parteien der Ausgangsverfahren ist das Verfahren ein Zwischenstreit in den bei den vorlegenden Gerichten anhängigen Rechtsstreitigkeiten; die Kostenentscheidung ist daher Sache dieser Gerichte. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

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

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

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.**

Unterschriften