Geschäftsverzeichnisnrn. 6590, 6597, 6599 und 6601
Entscheid Nr. 57/2021 vom 22. April 2021

E N T S C H E I D

In Sachen: Klagen auf Nichtigerklärung des Gesetzes vom 29. Mai 2016 « über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation », erhoben von der Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften, von der VoG « Académie Fiscale » und Jean Pierre Riquet, von der VoG « Liga voor Mensenrechten » und der VoG « Ligue des Droits de l'Homme » und von Patrick Van Assche und anderen.

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten F. Daoût und L. Lavrysen, und den Richtern J.-P. Moerman, T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman, M. Pâques und Y. Kherbache, unter Assistenz des Kanzlers F. Meersschaut, unter dem Vorsitz des Präsidenten F. Daoût,

erlässt nach Beratung folgenden Entscheid:

*

* *

I. *Gegenstand der Klagen und Verfahren*

a. Mit einer Klageschrift, die dem Gerichtshof mit am 10. Januar 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 11. Januar 2017 in der Kanzlei eingegangen ist, erhob die Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften, unterstützt und vertreten durch RA E. Lemmens und RA J.-F. Henrotte, in Lüttich zugelassen, Klage auf Nichtigerklärung des Gesetzes vom 29. Mai 2016 « über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation » (veröffentlicht im *Belgischen Staatsblatt* vom 18. Juli 2016).

b. Mit einer Klageschrift, die dem Gerichtshof mit am 16. Januar 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 17. Januar 2017 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung desselben Gesetzes: die VoG « Académie Fiscale » und Jean Pierre Riquet.

c. Mit einer Klageschrift, die dem Gerichtshof mit am 17. Januar 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 18. Januar 2017 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung desselben Gesetzes: die VoG « Liga voor Mensenrechten », unterstützt und vertreten durch RA J. Vander Velpen, in Antwerpen zugelassen, und die VoG « Ligue des Droits de l'Homme », unterstützt und vertreten durch RA R. Jespers, in Antwerpen zugelassen.

d. Mit einer Klageschrift, die dem Gerichtshof mit am 18. Januar 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 19. Januar 2017 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung desselben Gesetzes: Patrick Van Assche, Christel Van Akeleyen und Karina De Hoog, unterstützt und vertreten durch RA D. Pattyn, in Westflandern zugelassen.

Diese unter den Nummern 6590, 6597, 6599 und 6601 ins Geschäftsverzeichnis des Gerichtshofes eingetragenen Rechtssachen wurden verbunden.

In seinem Zwischenentscheid Nr. 96/2018 vom 19. Juli 2018, veröffentlicht im *Belgischen Staatsblatt* vom 27. Dezember 2018, hat der Verfassungsgerichtshof dem Gerichtshof der Europäischen Union folgende Vorabentscheidungsfragen gestellt:

« 1. Ist Artikel 15 Absatz 1 der Richtlinie 2002/58/EG in Verbindung mit dem Recht auf Sicherheit, das durch Artikel 6 der Charta der Grundrechte der Europäischen Union garantiert wird, und dem Recht auf Schutz der personenbezogenen Daten, wie es durch die Artikel 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union 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/EG 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 Artikel 23

Absatz 1 der Verordnung (EU) 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 Artikel 15 Absatz 1 der Richtlinie 2002/58/EG in Verbindung mit den Artikeln 4, 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union 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/EG 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 von Artikel 4 und 8 der Charta obliegen, und die darin besteht, 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 über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation 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? ».

In seinem Urteil vom 6. Oktober 2020 in den Rechtssachen C-511/18, C-512/18 und C-520/18 hat der Gerichtshof der Europäischen Union auf die Fragen geantwortet.

Durch Anordnung vom 21. Oktober 2020 hat der Gerichtshof nach Anhörung der referierenden Richter M. Pâques und T. Merckx-Van Goey beschlossen,

- die Verhandlung wiederzueröffnen,

- die Parteien aufzufordern, in einem spätestens am 23. November 2020 einzureichenden und innerhalb derselben Frist den jeweils anderen Parteien zu übermittelnden Ergänzungsschriftsatz ihren Standpunkt zu den Auswirkungen des vorerwähnten Urteils des Gerichtshofes der Europäischen Union auf die vorliegenden Rechtssachen darzulegen,

- dass keine Sitzung abgehalten wird, außer wenn eine Partei innerhalb von sieben Tagen nach Erhalt der Notifizierung dieser Anordnung einen Antrag auf Anhörung eingereicht hat, und

- dass vorbehaltlich eines solchen Antrags die Verhandlung am 25. November 2020 geschlossen und die Rechtssachen zur Beratung gestellt werden.

Ergänzungsschriftsätze wurden eingereicht von

- der klagenden Partei in der Rechtssache Nr. 6590,

- den klagenden Parteien in der Rechtssache Nr. 6599,

- den klagenden Parteien in der Rechtssache Nr. 6601,

- dem Ministerrat, unterstützt und vertreten durch RA E. de Lophem und RA S. Depré, in Brüssel zugelassen (in den Rechtssachen Nrn. 6590 und 6597),

- dem Ministerrat, unterstützt und vertreten durch RA J. Vanpraet, in Westflandern zugelassen (in den Rechtssachen Nrn. 6599 und 6601),

Infolge der Anträge mehrerer Parteien auf Anhörung hat der Gerichtshof durch Anordnung vom 12. November 2020 den Sitzungstermin auf den 9. Dezember 2020 anberaumt.

Auf der öffentlichen Sitzung vom 9. Dezember 2020

- erschienen

. RÄin E. Kiehl, in Lüttich zugelassen, *loco* RA E. Lemmens, und RA J.-F. Henrotte, für die klagende Partei in der Rechtssache Nr. 6590,

. RA R. Jespers und RA J. Fermon, in Brüssel zugelassen, für die klagenden Parteien in der Rechtssache Nr. 6599,

. RA D. Pattyn, für die klagenden Parteien in der Rechtssache Nr. 6601,

. RA E. de Lophem, ebenfalls *loco* RA S. Depré, für den Ministerrat (in den Rechtssachen Nrn. 6590 und 6597),

. RA J. Vanpraet, für den Ministerrat (in den Rechtssachen Nrn. 6599 und 6601),

- haben die referierenden Richter M. Pâques und T. Merckx-Van Goey Bericht erstattet,

- wurden die vorgenannten Rechtsanwälte angehört,

- wurden die Rechtssachen zur Beratung gestellt.

Die Vorschriften des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, die sich auf das Verfahren und den Sprachengebrauch beziehen, wurden zur Anwendung gebracht.

II. *Rechtliche Würdigung*

(…)

In Bezug auf das angefochtene Gesetz und seinen Kontext

B.1. Die klagenden Parteien beantragen die Nichtigerklärung des Gesetzes vom 29. Mai 2016 « über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation », das bestimmt:

« KAPITEL 1 - *Allgemeine Bestimmung*

Artikel 1 - Vorliegendes Gesetz regelt eine in Artikel 74 der Verfassung erwähnte Angelegenheit.

KAPITEL 2 - *Abänderungen des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation*

Art. 2 - Artikel 2 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation, zuletzt abgeändert durch das Gesetz vom 18. Dezember 2015 und teilweise für nichtig erklärt durch Entscheid Nr. 84/2015 des Verfassungsgerichtshofes, wird wie folgt abgeändert:

a) Nummer 11 wird wie folgt ersetzt:

‘ 11. " Betreibern ": Personen, die verpflichtet sind, eine Meldung gemäß Artikel 9 einzureichen, ’.

b) Anstelle von Nr. 74, für nichtig erklärt durch Entscheid Nr. 84/2015 des Verfassungsgerichtshofes, wird eine Nr. 74 mit folgendem Wortlaut eingefügt:

‘ 74. " erfolglosen Anrufversuchen ": Telefonanrufe, bei denen die Verbindung erfolgreich aufgebaut wurde, die aber unbeantwortet geblieben sind, oder bei denen das Netzwerkmanagement eingegriffen hat, ’.

Art. 3 - Artikel 125 § 2 desselben Gesetzes wird aufgehoben.

Art. 4 - In dasselbe Gesetz wird anstelle von Artikel 126, für nichtig erklärt durch Entscheid Nr. 84/2015 des Verfassungsgerichtshofes, ein Artikel 126 mit folgendem Wortlaut eingefügt:

‘ Art. 126 - § 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 einer 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 Strafprozessgesetzbuches 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 Instituts 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 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.

§ 4 - Für die Vorratsspeicherung der in § 3 erwähnten Daten gilt für in § 1 Absatz 1 erwähnte Anbieter und Betreiber Folgendes:

1. Sie gewährleisten, dass die auf Vorrat gespeicherten Daten von der gleichen Qualität sind und der gleichen Sicherheit und dem gleichen Schutz unterliegen wie die im Netz vorhandenen Daten.

2. Sie sorgen dafür, dass in Bezug auf die auf Vorrat gespeicherten Daten geeignete technische und organisatorische Maßnahmen getroffen werden, um sie vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung, unbefugter oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen.

3. Sie gewährleisten, dass der Zugang zu den auf Vorrat gespeicherten Daten ausschließlich einem oder mehreren Mitgliedern des in Artikel 126/1 § 1 erwähnten Koordinationsbüros vorbehalten ist.

4. Sie speichern die Daten auf Vorrat auf dem Gebiet der Europäischen Union.

5. Sie treffen Maßnahmen zum technologischen Schutz, die die auf Vorrat gespeicherten Daten ab ihrer Registrierung für Personen, die nicht zu ihrem Zugang befugt sind, unlesbar und unbrauchbar machen.

6. Sie sorgen dafür, dass unbeschadet der Artikel 122 und 123 nach Ablauf der in § 3 erwähnten auf diese Daten anwendbaren Vorratsspeicherungsfrist die auf Vorrat gespeicherten Daten von den Trägern entfernt werden.

7. Sie sorgen dafür, dass bei Anträgen auf Erhalt auf Vorrat gespeicherter Daten seitens einer in § 2 erwähnten Behörde die Nutzung dieser Daten rückverfolgt werden kann.

Die in Absatz 1 Nr. 7 erwähnte Rückverfolgbarkeit wird mit Hilfe eines Tagebuchs durchgeführt. Das Institut und der Ausschuss für den Schutz des Privatlebens dürfen dieses Tagebuch einsehen oder eine Kopie des gesamten oder eines Teils dieses Tagebuchs verlangen. Das Institut und der Ausschuss für den Schutz des Privatlebens schließen ein Zusammenarbeitsprotokoll über Kenntnisnahme und Kontrolle des Inhalts des Tagebuchs.

§ 5 - Der Minister und der Minister der Justiz sorgen dafür, dass der Abgeordnetenkammer jährlich eine Statistik über die Vorratsspeicherung der Daten übermittelt wird, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste beziehungsweise öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden.

Aus dieser Statistik muss hervorgehen:

1. in welchen Fällen gemäß den anwendbaren gesetzlichen Bestimmungen Daten an die zuständigen Behörden weitergegeben worden sind,

2. wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der zuständigen Behörde angefordert wurden, vergangen ist,

3. in welchen Fällen die Anfragen nach Daten ergebnislos geblieben sind.

Diese Statistik darf keine personenbezogenen Daten enthalten.

Die Daten, die die Anwendung von § 2 Nr. 1 betreffen, werden ebenfalls dem Bericht beigefügt, den der Minister der Justiz gemäß Artikel 90*decies* des Strafprozessgesetzbuches dem Parlament erstatten muss.

Der König legt auf Vorschlag des Ministers der Justiz und des Ministers nach Stellungnahme des Instituts die Statistik fest, die in § 1 Absatz 1 erwähnte Anbieter und Betreiber jährlich dem Institut übermitteln, und die Statistik, die das Institut dem Minister und dem Minister der Justiz übermittelt.

§ 6 - Unbeschadet des in § 5 Absatz 4 erwähnten Berichts erstatten der Minister und der Minister der Justiz der Abgeordnetenkammer zwei Jahre nach Inkrafttreten des in § 3 Absatz 4 erwähnten Königlichen Erlasses einen Evaluationsbericht über die Umsetzung des vorliegenden Artikels, damit überprüft wird, ob Bestimmungen angepasst werden müssen, insbesondere was die auf Vorrat zu speichernden Daten und die Vorratsspeicherungsfrist betrifft. ’

Art. 5 - In dasselbe Gesetz wird ein Artikel 126/1 mit folgendem Wortlaut eingefügt:

"Art. 126/1 - § 1 - Bei jedem in Artikel 126 § 1 Absatz 1 erwähnten Betreiber und Anbieter wird ein Koordinationsbüro eingerichtet, das beauftragt ist, den gesetzlich befugten belgischen Behörden auf deren Antrag hin aufgrund von Artikel 122, 123 und 126 auf Vorrat gespeicherte Daten, Identifizierungsdaten des Anrufers aufgrund von Artikel 107 § 2 Absatz 1 oder Daten, die aufgrund der Artikel 46*bis*, 88*bis* und 90*ter* des Strafprozessgesetzbuches und der Artikel 18/7, 18/8, 18/16 und 18/17 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten und Sicherheitsdienste angefordert werden können, zu übermitteln.

Gegebenenfalls können mehrere Betreiber oder Anbieter ein gemeinsames Koordinationsbüro schaffen. In diesem Fall muss das Koordinationsbüro denselben Dienst für jeden Betreiber oder Anbieter vorsehen.

Um dem Koordinationsbüro anzugehören müssen die Mitglieder:

1. Inhaber einer positiven und nicht abgelaufenen Sicherheitsstellungnahme gemäß Artikel 22*quinquies* des Gesetzes vom 11. Dezember 1998 über die Klassifizierung und die Sicherheitsermächtigungen, -bescheinigungen und -stellungnahmen sein,

2. nicht von einer Verweigerung durch den Justizminister betroffen sein; eine solche Verweigerung muss mit Gründen versehen sein und kann jederzeit eintreten.

Eine Stellungnahme wird fünf Jahre nach ihrer Abgabe als abgelaufen betrachtet.

Betreiber und Anbieter, die keinen der in Artikel 126 § 1 erwähnten Dienste anbieten, werden von der in Absatz 3 Nr. 1 erwähnten Bedingung befreit.

Nur die Mitglieder des Koordinationsbüros dürfen Anträge der Behörden in Bezug auf die in Absatz 1 erwähnten Daten beantworten. Sie dürfen jedoch unter ihrer Aufsicht und auf das Notwendigste beschränkt von Angestellten von Betreiber oder Anbieter technische Hilfe bekommen.

Mitglieder des Koordinationsbüros und Angestellte, die technische Hilfe leisten, unterliegen dem Berufsgeheimnis.

In Artikel 126 § 1 Absatz 1 erwähnte Betreiber und Anbieter achten auf die Vertraulichkeit der vom Koordinationsbüro verarbeiteten Daten und teilen dem Institut und Ausschuss für den Schutz des Privatlebens die Kontaktdaten des Koordinationsbüros und seiner Mitglieder und jede Änderung dieser Daten unverzüglich mit.

§ 2 - In Artikel 126 § 1 Absatz 1 erwähnte Betreiber und Anbieter richten interne Verfahren zur Beantwortung von Anfragen über den Zugang der Behörden zu den personenbezogenen Daten der Nutzer ein. Sie stellen dem Institut auf Anfrage Informationen über diese Verfahren, die Zahl der eingegangenen Anfragen, die vorgebrachten rechtlichen Begründungen und ihre Antworten zur Verfügung.

In Artikel 126 § 1 Absatz 1 erwähnte Betreiber und Anbieter gelten für die aufgrund von Artikel 126 und des vorliegenden Artikels verarbeiteten Daten als für die Verarbeitung Verantwortliche im Sinne des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten.

Betreiber öffentlicher elektronischer Kommunikationsnetze und Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt halten für den Zugang zu den in § 1 erwähnten Daten und ihre Übermittlung an die Behörden Artikel 114 § 2 ein.

§ 3 - In Artikel 126 § 1 Absatz 1 erwähnte Betreiber und Anbieter bestimmen einen oder mehrere Beauftragte für den Schutz personenbezogener Daten, der beziehungsweise die die in § 1 Absatz 3 erwähnten kumulativen Bedingungen erfüllen muss.

Dieser Beauftragte darf nicht dem Koordinationsbüro angehören.

Verschiedene Betreiber oder Anbieter dürfen einen oder mehrere gemeinsame Beauftragte für den Schutz personenbezogener Daten bestimmen. In diesem Fall dürfen diese Beauftragte denselben Auftrag für jeden individuellen Betreiber oder Anbieter ausführen.

Bei der Ausführung seiner Aufträge handelt der Beauftragte für den Schutz personenbezogener Daten vollkommen unabhängig und hat Zugang zu allen personenbezogenen Daten, die den Behörden übermittelt werden, und zu allen relevanten Räumlichkeiten von Anbieter und Betreiber.

Die Ausführung seiner Aufträge darf für den Beauftragten keine Nachteile mit sich bringen. Er darf insbesondere als Beauftragter aufgrund der Ausführung der Aufgaben, die ihm anvertraut sind, nicht ohne eingehende Begründung entlassen oder ersetzt werden.

Der Beauftragte muss die Möglichkeit haben, direkt mit dem Betreiber oder Anbieter zu kommunizieren.

Der Beauftragte für den Schutz personenbezogener Daten sorgt dafür, dass:

1. vom Koordinationsbüro durchgeführte Verarbeitungen gemäß dem Gesetz ausgeführt werden,

2. Anbieter oder Betreiber nur Daten sammelt und speichert, die er auch gesetzlich aufbewahren darf,

3. nur gesetzlich befugte Behörden Zugang zu den gespeicherten Daten haben,

4. Sicherheitsmaßnahmen und Maßnahmen zum Schutz von personenbezogenen Daten, die in vorliegendem Gesetz und in der Sicherheitspolitik von Anbieter und Betreiber beschrieben sind, durchgeführt werden.

In Artikel 126 § 1 Absatz 1 erwähnte Anbieter und Betreiber teilen dem Institut und dem Ausschuss für den Schutz des Privatlebens die Kontaktdaten der Beauftragten für den Schutz personenbezogener Daten und jede Änderung dieser Daten unverzüglich mit.

§ 4 - Der König bestimmt durch einen im Ministerrat beratenen Erlass nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts:

1. Modalitäten für Beantragung und Abgabe der Sicherheitsstellungnahme,

2. Anforderungen, die das Koordinationsbüro erfüllen muss, unter Berücksichtigung der Situation von Betreiber und Anbieter, die wenige Anträge von Gerichtsbehörden erhalten, die keine Niederlassung in Belgien haben oder hauptsächlich im Ausland tätig sind,

3. Informationen, die dem Institut und Ausschuss für den Schutz des Privatlebens gemäß den Paragraphen 1 und 3 zu übermitteln sind, und Behörden, die Zugang zu diesen Informationen haben,

4. andere Regeln für die Zusammenarbeit der in Artikel 126 § 1 Absatz 1 erwähnten Betreiber und Anbieter mit den belgischen Behörden oder bestimmten unter ihnen für die Übermittlung der in § 1 erwähnten Daten, gegebenenfalls einschließlich Form und Inhalt des Antrags pro betroffene Behörde. ’

Art. 6 - Artikel 127 desselben Gesetzes, abgeändert durch die Gesetze vom 4. Februar 2010, 10. Juli 2012 und 27. März 2014, wird wie folgt abgeändert:

1. Paragraph 1 wird wie folgt abgeändert:

a) In Absatz 1 werden zwischen dem Wort ‘ Betreibern ’ und den Wörtern ‘ und Endnutzern ’ die Wörter ‘ Anbietern wie in Artikel 126 § 1 Absatz 1 erwähnt ’ eingefügt.

b) In Absatz 2 werden zwischen dem Wort ‘ Betreiber ’ und den Wörtern ‘ an den in Absatz 1 Nr. 2 erwähnten Handlungen ’ die Wörter ‘ und Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt ’ eingefügt.

2. Paragraph 6 wird aufgehoben.

Art. **7 - A**rtikel 145 desselben Gesetzes, abgeändert durch die Gesetze vom 25. April 2007 und 27. März 2014, wird wie folgt abgeändert:

1. Zwischen dem Wort ‘ 124, ’ und dem Wort ‘ 127 ’ werden die Wörter ‘ 126, 126/1, ’ eingefügt.

2. Zwischen dem Wort ‘ 47 ’ und den Wörtern ‘ und 127 ’ werden die Wörter ‘ , 126, 126/1 ’ eingefügt.

3. Anstelle von § 3*ter*, für nichtig erklärt durch Entscheid Nr. 84/2015 des Verfassungsgerichtshofes, wird ein § 3*ter* mit folgendem Wortlaut eingefügt:

‘ § 3*ter* - Mit einer Geldbuße von 50 bis zu 50.000 EUR und einer Gefängnisstrafe von sechs Monaten bis zu drei Jahren oder mit nur einer dieser Strafen wird belegt:

1. wer in anderen als in den durch das Gesetz vorgesehenen Fällen oder unter Nichteinhaltung der durch das Gesetz vorgeschriebenen Formalitäten bei der Ausübung seiner Funktion in betrügerischer Absicht oder mit der Absicht zu schaden die in Artikel 126

erwähnten Daten auf irgendeine Weise übernimmt, in Besitz hält oder von diesen Daten irgendeinen Gebrauch macht,

2. wer Daten, wohl wissend, dass sie durch Begehung der in Nr. 1 erwähnten Straftat erhalten wurden, in Besitz hält, anderen Personen preisgibt oder verbreitet oder von ihnen irgendeinen Gebrauch macht. ’

KAPITEL 3 - *Abänderungen des Strafprozessgesetzbuches*

Art. 8 - Artikel 46*bis* § 1 des Strafprozessgesetzbuches, eingefügt durch das Gesetz vom 10. Juni 1998 und ersetzt durch das Gesetz vom 23. Januar 2007, wird wie folgt abgeändert:

a) [Abänderung des französischen Textes]

b) Der Paragraph wird durch einen Absatz mit folgendem Wortlaut ergänzt:

‘ Für Straftaten, die keine Hauptkorrektionalgefängnisstrafe von einem Jahr oder keine schwerere Strafe zur Folge haben können, kann der Prokurator des Königs oder, in Fällen äußerster Dringlichkeit, der Gerichtspolizeioffizier die in Absatz 1 erwähnten Daten nur für einen Zeitraum von sechs Monaten vor seiner Entscheidung anfordern. ’

Art. 9 - Artikel 88*bis* desselben Gesetzbuches, eingefügt durch das Gesetz vom 11. Februar 1991, ersetzt durch das Gesetz vom 10. Juni 1998 und abgeändert durch die Gesetze vom 8. Juni 2008 und 27. Dezember 2012, wird wie folgt abgeändert:

a) Paragraph 1 Absatz 1 wird wie folgt ersetzt:

‘ Wenn es schwerwiegende Indizien dafür gibt, dass die Straftaten eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben können, und wenn der Untersuchungsrichter der Meinung ist, dass es Umstände gibt, die die Erfassung von elektronischen Nachrichten oder die Lokalisierung der Herkunft oder der Bestimmung von elektronischen Nachrichten notwendig machen, um die Wahrheit herauszufinden, kann er, nötigenfalls indem er dazu direkt oder über einen vom König bestimmten Polizeidienst die technische Mitwirkung des Betreibers eines elektronischen Kommunikationsnetzes oder des Anbieters eines elektronischen Kommunikationsdienstes anfordert, Folgendes vornehmen oder vornehmen lassen:

1. die Erfassung der Verkehrsdaten von elektronischen Kommunikationsmitteln, von denen elektronische Nachrichten ausgehen oder ausgingen beziehungsweise an die elektronische Nachrichten gerichtet sind oder waren,

2. die Lokalisierung der Herkunft oder der Bestimmung von elektronischen Nachrichten. ’

b) In § 1 Absatz 2 wird das Wort ‘ Telekommunikationsmittel ’ durch die Wörter ‘ elektronische Kommunikationsmittel ’ ersetzt und werden die Wörter ‘ der Fernmeldeverbindung ’ jeweils durch die Wörter ‘ der elektronischen Nachricht ’ ersetzt.

c) Paragraph 1 Absatz 3 wird wie folgt ersetzt:

‘ Der Untersuchungsrichter gibt die tatsächlichen Umstände der Sache, die die Maßnahme rechtfertigen, deren Verhältnismäßigkeit unter Berücksichtigung des Privatlebens und deren Subsidiarität gegenüber jeder anderen Ermittlungsaufgabe in einem mit Gründen versehenen Beschluss an. ’

d) Paragraph 1 Absatz 4 wird wie folgt ersetzt:

‘ Er gibt auch die Dauer der Maßnahme für die Zukunft an, die nicht länger als zwei Monate ab dem Beschluss betragen darf, unbeschadet einer Erneuerung, und gegebenenfalls den Zeitraum in der Vergangenheit, über den der Beschluss sich gemäß § 2 erstreckt. ’

e) Paragraph 1 wird durch einen Absatz mit folgendem Wortlaut ergänzt:

‘ Im Dringlichkeitsfall kann die Maßnahme mündlich angeordnet werden. Sie muss so schnell wie möglich in der in den Absätzen 3 und 4 vorgesehenen Form bestätigt werden. ’

f) Paragraph 2, dessen heutiger Text § 4 wird, wird wie folgt ersetzt:

‘ § 2 - In Bezug auf die Anwendung der in § 1 Absatz 1 erwähnten Maßnahme auf die Verkehrs- oder Standortdaten, die aufgrund von Artikel 126 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation gespeichert werden, gelten folgende Bestimmungen:

- Für eine in Buch II Titel I*ter* des Strafgesetzbuches erwähnte Straftat kann der Untersuchungsrichter in seinem Beschluss die Daten für einen Zeitraum von zwölf Monaten vor dem Beschluss anfordern.

- Für eine andere in Artikel 90*ter* §§ 2 bis 4 erwähnte Straftat, die nicht im ersten Gedankenstrich erwähnt ist, oder für eine Straftat, die im Rahmen einer in Artikel 324*bis* des Strafgesetzbuches erwähnten kriminellen Organisation begangen worden ist, oder für eine Straftat, die eine Hauptkorrektionalgefängnisstrafe von fünf Jahren oder eine schwerere Strafe zur Folge haben kann, kann der Untersuchungsrichter in seinem Beschluss die Daten für einen Zeitraum von neun Monaten vor dem Beschluss anfordern.

- Für andere Straftaten kann der Untersuchungsrichter die Daten nur für einen Zeitraum von sechs Monaten vor dem Beschluss anfordern. ’

g) Der Artikel wird durch einen Paragraphen 3 mit folgendem Wortlaut ergänzt:

‘ § 3 - Die Maßnahme darf sich nur dann auf elektronische Kommunikationsmittel eines Rechtsanwalts oder Arztes beziehen, wenn dieser selber verdächtigt wird, eine in § 1 erwähnte Straftat begangen zu haben oder daran beteiligt gewesen zu sein, oder wenn genaue Tatsachen vermuten lassen, dass Dritte, die verdächtigt werden, eine in § 1 erwähnte Straftat begangen zu haben, seine elektronischen Kommunikationsmittel benutzen.

Die Maßnahme darf nicht durchgeführt werden, ohne dass - je nach Fall - der Präsident der Rechtsanwaltskammer oder der Vertreter der provinzialen Ärztekammer davon in Kenntnis gesetzt worden ist. Dieselben Personen werden vom Untersuchungsrichter darüber in Kenntnis

gesetzt, welche Elemente seiner Meinung nach unter das Berufsgeheimnis fallen. Diese Elemente werden nicht im Protokoll festgehalten. ’

h) In § 2, der zu § 4 umnummeriert wird, werden in Absatz 1 die Wörter ‘ Jeder Betreiber eines Telekommunikationsnetzes und jeder Anbieter einer Telekommunikationsdienstleistung ’ durch die Wörter ‘ Jeder Betreiber eines elektronischen Kommunikationsnetzes und jeder Anbieter eines elektronischen Kommunikationsdienstes ’ ersetzt.

Art. 10 - Artikel 90*decies* desselben Gesetzbuches, eingefügt durch das Gesetz vom 30. Juni 1994 und abgeändert durch die Gesetze vom 8. April 2002, 7. Juli 2002, 6. Januar 2003 und durch das Gesetz vom 30. Juli 2013, für nichtig erklärt durch den Entscheid Nr. 84/2015 des Verfassungsgerichtshofes, wird durch einen Absatz mit folgendem Wortlaut ergänzt:

‘ Diesem Bericht wird ebenfalls der in Anwendung von Artikel 126 § 5 Absatz 4 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation erstellte Bericht beigefügt. ’

Art. 11 - In Artikel 464/25 § 2 Absatz 1 desselben Gesetzbuches werden die Wörter ‘ Artikel 88*bis* § 2 Absatz 1 und 3 ’ durch die Wörter ‘ Artikel 88*bis* § 4 Absatz 1 und 3 ’ ersetzt.

KAPITEL 4 - *Abänderungen des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste*

Art. 12 - Artikel 13 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste, abgeändert durch das Gesetz vom 4. Februar 2010, wird wie folgt abgeändert:

1. *[Abänderung des niederländischen Textes]*

2. Absatz 3 wird wie folgt ersetzt:

‘ Die Nachrichten- und Sicherheitsdienste sorgen für die Sicherheit der Angaben, die sich auf ihre Quellen beziehen, und der von diesen Quellen gelieferten Informationen und personenbezogenen Daten. ’

3. Der Artikel wird durch einen Absatz mit folgendem Wortlaut ergänzt:

‘ Die Bediensteten der Nachrichten- und Sicherheitsdienste haben Zugang zu den von ihrem Dienst gesammelten und verarbeiteten Informationen, Auskünfte und personenbezogenen Daten, sofern diese bei der Ausübung ihrer Funktion oder ihres Auftrags nützlich sind. ’

Art. 13 - Artikel 18/3 desselben Gesetzes, eingefügt durch das Gesetz vom 4. Februar 2010, wird wie folgt abgeändert:

a) Der heutige Paragraph 1 Absatz 3 wird Paragraph 5.

b) In § 1 Absatz 4, der § 7 wird, werden die Wörter ‘ um die spezifische Methode zum Sammeln von Daten anzuwenden ’ durch die Wörter ‘ um die Anwendung der spezifischen Methode zum Sammeln von Daten zu überwachen ’ ersetzt.

c) Paragraph 2, dessen heutige Absätze 2 bis 5 § 6 werden, wird wie folgt ersetzt:

‘ § 2 - Die Entscheidung des Dienstleiters enthält Folgendes:

1. die Art der spezifischen Methode,

2. je nach Fall, die natürlichen oder juristischen Personen, Vereinigungen oder Gruppierungen, Gegenstände, Orte, Ereignisse oder Informationen, die Gegenstand der spezifischen Methode sind,

3. die potentielle Gefahr, die die spezifische Methode rechtfertigt,

4. die tatsächlichen Umstände, die die spezifische Methode rechtfertigen, die Begründung in Sachen Subsidiarität und Verhältnismäßigkeit, einschließlich der Verbindung zwischen Nr. 2 und 3,

5. den Zeitraum ab der Notifizierung der Entscheidung an den Ausschuss, in dem die spezifische Methode angewandt werden kann,

6. den Namen des Nachrichtenoffiziers (der Nachrichtenoffiziere), der (die) für die Überwachung der Anwendung der spezifischen Methode verantwortlich ist (sind),

7. gegebenenfalls, das technische Mittel, das bei der Anwendung der spezifischen Methode benutzt wird,

8. gegebenenfalls, das Zusammentreffen mit einem Ermittlungsverfahren oder einer gerichtlichen Untersuchung,

9. gegebenenfalls, die ernstzunehmenden Indizien dafür, dass der Rechtsanwalt, der Arzt oder der Journalist persönlich und aktiv an der Entstehung oder der Entwicklung der potentiellen Gefahr mitwirkt oder mitgewirkt hat,

10. in dem Fall, in dem Artikel 18/8 Anwendung findet, die Begründung der Dauer des Zeitraums, auf den die Sammlung der Daten bezogen ist,

11. das Datum der Entscheidung,

12. die Unterschrift des Dienstleiters. ’

d) Paragraph 3 wird wie folgt ersetzt:

‘ § 3 - Für jede spezifische Methode wird dem Ausschuss am Ende jedes Monats eine Liste der ausgeführten Maßnahmen übermittelt.

Diese Listen umfassen die in § 2 Nr. 1 bis 3, 5 und 7 aufgeführten Daten. ’

e) Der Artikel wird durch einen Paragraphen 8 mit folgendem Wortlaut ergänzt:

‘ § 8 - Der Dienstleiter beendet die spezifische Methode, wenn die potentielle Gefahr, die die Methode gerechtfertigt hat, nicht mehr besteht, wenn die Methode für den Zweck, für den sie angewandt worden ist, nicht mehr nützlich ist oder wenn er eine Rechtsverletzung festgestellt hat. Er setzt den Ausschuss schnellstmöglich von seiner Entscheidung in Kenntnis. ’

Art. 14 - Artikel 18/8 desselben Gesetzes, eingefügt durch das Gesetz vom 4. Februar 2010, wird wie folgt abgeändert:

a) Paragraph 1 Absatz 3 wird wie folgt ersetzt:

‘ Die Nachrichten- und Sicherheitsdienste können im Interesse der Erfüllung ihrer Aufträge, notfalls indem sie dazu die technische Mitwirkung des Betreibers eines elektronischen Kommunikationsnetzes oder des Anbieters eines elektronischen Kommunikationsdienstes anfordern, Folgendes vornehmen oder vornehmen lassen:

1. die Erfassung der Verkehrsdaten von elektronischen Kommunikationsmitteln, von denen elektronische Nachrichten ausgehen oder ausgingen beziehungsweise an die elektronische Nachrichten gerichtet sind oder waren,

2. die Lokalisierung der Herkunft oder der Bestimmung von elektronischen Nachrichten. ’

b) In § 1 Absatz 2 wird das Wort ‘ Verbindungsdaten ’ durch das Wort ‘ Verkehrsdaten ’ ersetzt.

c) Paragraph 2, dessen heutiger Text § 4 wird, wird wie folgt ersetzt:

‘ § 2 - In Bezug auf die Anwendung der in § 1 erwähnten Methode auf die Daten, die aufgrund von Artikel 126 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation gespeichert werden, gelten folgende Bestimmungen:

1. Für eine potentielle Gefahr, die sich auf eine Aktivität mit möglichem Bezug zu kriminellen Organisationen oder schädlichen sektiererischen Organisationen bezieht, kann der Dienstleiter in seiner Entscheidung die Daten nur für einen Zeitraum von sechs Monaten vor der Entscheidung anfordern.

2. Für eine potentielle Gefahr, die nicht in Nr. 1 und Nr. 3 erwähnt ist, kann der Dienstleiter in seiner Entscheidung die Daten für einen Zeitraum von neun Monaten vor der Entscheidung anfordern.

3. Für eine potentielle Gefahr, die sich auf eine Aktivität mit möglichem Bezug zu Terrorismus oder Extremismus bezieht, kann der Dienstleiter in seiner Entscheidung die Daten für einen Zeitraum von zwölf Monaten vor der Entscheidung anfordern. ’

Art. 15 - In Artikel 43/3 desselben Gesetzes, eingefügt durch das Gesetz vom 4. Februar 2010, werden die Wörter ‘ Artikel 18/3 § 2 ’ durch die Wörter ‘ Artikel 18/3 § 3 ’ ersetzt.

Art. 16 - In Artikel 43/5 § 1 Absatz 2 desselben Gesetzes werden die Wörter ‘ Artikel 18/3 § 2 ’ durch die Wörter ‘ Artikel 18/3 § 3 ’ ersetzt ».

B.2. Durch das angefochtene Gesetz wollte der Gesetzgeber der Nichtigerklärung von Artikel 126 des Gesetzes vom 13. Juni 2005 « über die elektronische Kommunikation » (nachstehend: Gesetz vom 13. Juni 2005), abgeändert durch das Gesetz vom 30. Juli 2013 « zur Abänderung der Artikel 2, 126 und 145 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation und des Artikels 90*decies* des Strafprozessgesetzbuches », durch den Entscheid Nr. 84/2015 des Gerichtshofes vom 11. Juni 2015 Rechnung tragen (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1567/001, S. 4).

B.3. Aus den Vorarbeiten zu dem angefochtenen Gesetz geht hervor, dass der Gesetzgeber sowohl den vorerwähnten Entscheid Nr. 84/2015 des Gerichtshofes vom 11. Juni 2015 als auch das Urteil des Gerichtshofes der Europäischen Union vom 8. April 2014 in den verbundenen Rechtssachen *Digital Rights Ireland Ltd* (C-293/12) und *Kärntner Landesregierung u.a.* (C-594/12), mit dem der Gerichtshof die 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/EG » für ungültig erklärt hat und auf dem der Entscheid Nr. 84/2015 beruht, gründlich geprüft hat.

Das Ziel, das der Gesetzgeber mit dem angefochtenen Gesetz verfolgt, ist nicht nur die Bekämpfung des Terrorismus und der Kinderpornographie, sondern auch die Möglichkeit, die auf Vorrat gespeicherten Daten in einer Vielzahl von Situationen, in denen diese Daten sowohl der Ausgangspunkt als auch eine Phase der strafrechtlichen Ermittlung sein können, zu benutzen (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1567/001, S. 6).

B.4. Aus der Begründung des angefochtenen Gesetzes geht hervor, dass der Gesetzgeber der Auffassung war, es sei im Lichte der Zielsetzung unmöglich, eine gezielte und differenzierte Vorratsspeicherungspflicht einzuführen, und sich dafür entschieden hat, die allgemeine und unterschiedslose Vorratsspeicherungspflicht mit strikten Garantien zu versehen, sowohl auf der Ebene des Schutzes der Aufbewahrung als auch auf der Ebene des Zugangs, um den Eingriff in das Recht auf Achtung des Schutzes des Privatlebens auf ein Minimum zu begrenzen. In diesem Zusammenhang wurde betont, dass es schlicht unmöglich sei, eine a priori-Differenzierung nach Personen, Zeiträumen und geografischen Gebieten vorzunehmen (ebenda, SS. 10-18).

Zur Hauptsache

B.5. Der einzige Klagegrund in den Rechtssachen Nrn. 6590 und 6597 ist aus einem Verstoß durch das angefochtene Gesetz gegen die Artikel 10 und 11 der Verfassung, an sich oder in Verbindung mit den Artikeln 6 und 8 der Europäischen Menschenrechtskonvention sowie mit den Artikeln 7, 8 und 47 der Charta der Grundrechte der Europäischen Union abgeleitet.

B.6.1. Die Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften, klagende Partei in der Rechtssache Nr. 6590, bemängelt an dem angefochtenen Gesetz, dass es die Nutzer der Telekommunikations- oder elektronischen Kommunikationsdienste, die dem Berufsgeheimnis unterliegen, darunter insbesondere Rechtsanwälte, und die anderen Nutzer dieser Dienste gleich behandele. Diese klagende Partei stellt fest, dass das Gesetz auch eine allgemeine Pflicht zur Aufzeichnung und Vorratsspeicherung von bestimmten Metadaten beinhalte, mit denen festgestellt werden könne, ob ein Rechtsanwalt von einer natürlichen oder juristischen Person um Rat gefragt worden sei, mit denen dieser Rechtsanwalt identifiziert werden könne, mit denen seine Gesprächspartner und insbesondere seine Klienten sowie das Datum und die Uhrzeit der Kommunikation identifiziert werden könnten. Diese allgemeine Pflicht werde sämtlichen öffentlichen Anbietern von Festnetztelefon-, Mobilfunk-, Internetzugangs-, Internet-E-Mail-, Internet-Telefonie-Diensten und von öffentlichen elektronischen Kommunikationsnetzen auferlegt.

B.6.2. Die klagende Partei in der Rechtssache Nr. 6590 kritisiert an dem angefochtenen Gesetz ebenfalls, eine allgemeine Vorratsspeicherungspflicht für Daten vorzusehen, ohne eine Unterscheidung der Rechtsunterworfenen danach vorzunehmen, ob sie Gegenstand einer Ermittlungs- oder Strafverfolgungsmaßnahme wegen Tatbeständen, die zu einer strafrechtlichen Verurteilung führen können, seien oder nicht. Sie führt weiter aus, dass die im Gesetz erwähnten Datenkategorien äußerst umfassend und vielfältig seien, insofern sie die Daten zur Identifizierung von Nutzern oder Teilnehmern und der Kommunikationsmittel, die Daten in Bezug auf Zugang und Verbindung der Endeinrichtung zu Netzwerk und Dienst und in Bezug auf den Standort dieser Ausrüstung, einschließlich des Netzabschlusspunktes sowie die Kommunikationsdaten betreffen würden, auch wenn ihr Inhalt ausgenommen sei.

B.7.1. Die klagenden Parteien in der Rechtssache Nr. 6597 werfen dem angefochtenen Gesetz vor, die Nutzer der Telekommunikations- oder elektronischen Kommunikationsdienste, die dem Berufsgeheimnis unterliegen, darunter insbesondere Wirtschafts- und Steuerprüfer, und die anderen Nutzer dieser Dienste gleich zu behandeln, ohne den besonderen Status von Wirtschafts- und Steuerprüfern, die grundlegende Bedeutung des Berufsgeheimnisses, dem sie unterliegen, und das notwendige Vertrauensverhältnis, das sie zu ihren Klienten haben müssten, zu berücksichtigen.

B.7.2. Sie bemängeln an dem angefochtenen Gesetz außerdem, dass es die Rechtsunterworfenen, die Gegenstand von Ermittlungs- oder Strafverfolgungsmaßnahmen wegen Tatbeständen sind, die unter die Zwecke der Vorratsspeicherung der strittigen elektronischen Daten fallen könnten, und die Rechtsunterworfenen, die nicht Gegenstand solcher Maßnahmen seien, gleich behandelt.

B.8.1. Der erste Klagegrund in der Rechtssache Nr. 6599 ist aus einem Verstoß gegen die Artikel 10, 11, 12, 15, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 8, 9, 10, 11, 14, 15, 17 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11 und 52 der Charta der Grundrechte der Europäischen Union, mit Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte, mit dem allgemeinen Grundsatz der Rechtssicherheit, der Verhältnismäßigkeit, des Rechts auf informationelle Selbstbestimmung sowie mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union, abgeleitet.

B.8.2. Die VoG « Liga voor Mensenrechten » und die VoG « Ligue des Droits de l'Homme » (nunmehr « Ligue des droits humains »), klagende Parteien in der Rechtssache Nr. 6599, werfen dem angefochtenen Gesetz vor, eine allgemeine Vorratsspeicherungspflicht für Daten vorzusehen, was die Betreiber und Anbieter von öffentlichen Telefondiensten (einschließlich der Internet-Telefonie), Internetzugangs- und Internet-E-Mail-Diensten sowie die Betreiber öffentlicher Kommunikationsnetze dazu verpflichte, *de facto* für alle Belgier, ob verdächtig oder nicht, die Verkehrsdaten in Bezug auf die Festnetztelefonie, die Mobilfunktelefonie und die Internet-Telefonie und die Daten in Bezug auf den Internetzugang zwölf Monate auf Vorrat zu speichern und sie der Polizei und der Justiz, den Nachrichten- und

Sicherheitsdiensten, den Hilfsdiensten, der Vermisstenzelle sowie dem Ombudsdienst für Telekommunikation zur Verfügung zu stellen.

B.9.1. Der erste Klagegrund in der Rechtssache Nr. 6601 ist aus einem Verstoß durch das angefochtene Gesetz gegen Artikel 8 der Europäischen Menschenrechtskonvention, die Artikel 7, 8, 11 Absatz 1 und 52 der Charta der Grundrechte der Europäischen Union, die Artikel 10, 11, 19 und 22 der Verfassung, Artikel 2 Buchstabe a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 « zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr » sowie die Artikel 1, 2, 3, 5, 6, 9 und 15 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 » (nachstehend: Richtlinie 2002/58/EG) abgeleitet.

B.9.2. Die klagenden Parteien in der Rechtssache Nr. 6601 sind natürliche Personen, die in Belgien wohnen und verschiedene elektronische Kommunikationsdienste im Rahmen eines mit einem Betreiber abgeschlossenen Vertrags nutzen. Im ersten Teil des ersten Klagegrunds bemängeln sie an dem angefochtenen Gesetz, dass es eine allgemeine und unterschiedslose Pflicht zur Aufbewahrung von Identifizierungs-, Verbindungs- und Standortdaten sowie persönliche Kommunikationsdaten zu Lasten der Anbieter von Telefoniediensten, auch über das Internet, von Internetzugangs-, Internet-E-Maildiensten, der Betreiber, die öffentliche Kommunikationsnetze bereitstellen, sowie der Betreiber, die einen dieser Dienste anbieten, vorsehe.

B.10. In Anbetracht ihres Zusammenhangs werden die in den verschiedenen Rechtssachen dargelegten Klagegründe zusammen geprüft.

B.11.1. Unter Berücksichtigung einerseits der unterschiedlichen Meinungen der klagenden Parteien und des Ministerrats darüber, wie verschiedene Bestimmungen auszulegen sind, insbesondere Artikel 15 Absatz 1 der Richtlinie 2002/58/EG und die Artikel 7, 8, 11 und 52 der Charta der Grundrechte der Europäischen Union, die der Gerichtshof in seine Kontrolle des angefochtenen Gesetzes einbeziehen muss, und andererseits der vom Ministerrat angeführten Erklärungen, um die Vereinbarkeit des angefochtenen Gesetzes mit den von den klagenden Parteien geltend gemachten Referenznormen zu rechtfertigen, hat der Gerichtshof

mit seinem Entscheid Nr. 96/2018 vom 19. Juli 2018 dem Gerichtshof der Europäischen Union die folgenden drei Vorabentscheidungsfragen gestellt:

« 1. Ist Artikel 15 Absatz 1 der Richtlinie 2002/58/EG in Verbindung mit dem Recht auf Sicherheit, das durch Artikel 6 der Charta der Grundrechte der Europäischen Union garantiert wird, und dem Recht auf Schutz der personenbezogenen Daten, wie es durch die Artikel 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union 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/EG 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 Artikel 23 Absatz 1 der Verordnung (EU) 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 Artikel 15 Absatz 1 der Richtlinie 2002/58/EG in Verbindung mit den Artikeln 4, 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union 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/EG 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 von Artikel 4 und 8 der Charta obliegen, und die darin besteht, 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 über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation 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? ».

B.11.2. Artikel 15 Absatz 1 der Richtlinie 2002/58/EG bestimmt:

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

B.11.3. Der Gerichtshof hat ebenfalls entschieden, die Prüfung der Rechtssachen auszusetzen, bis der Gerichtshof der Europäischen Union ein Urteil in den Rechtssachen *Ministerio Fiscal* (C-207/16) und *Privacy International gegen Secretary of State for Foreign and Commonwealth Affairs u.a.* (C-623/17) gefällt hat.

B.12. Mit ihrem Urteil vom 2. Oktober 2018 in der Rechtssache *Ministerio Fiscal* (C-207/16) hat die Große Kammer des Gerichtshofes entschieden, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7 und 8 der Charta dahin auszulegen ist, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta der Grundrechte der Europäischen Union verankerte Grundreche darstellt, der nicht so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste. Dieses Urteil beruht auf der folgenden Begründung:

« *Zur Beantwortung der Fragen*

48. Mit seinen beiden Fragen, die zusammen zu prüfen sind, möchte das vorlegende Gericht wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 der Charta dahin auszulegen ist, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta verankerte Grundreche darstellt, der so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden

müsste, und nach welchen Kriterien bejahendenfalls die Schwere der in Rede stehenden Straftat zu beurteilen ist.

49. Insoweit geht, wie der Generalanwalt in Nr. 38 seiner Schlussanträge ausgeführt hat, aus dem Vorabentscheidungsersuchen hervor, dass mit diesem nicht geklärt werden soll, ob die im Ausgangsverfahren in Rede stehenden personenbezogenen Daten von den Betreibern elektronischer Kommunikationsdienste unter Beachtung der in Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 der Charta vorgesehenen Voraussetzungen gespeichert wurden. Das Ersuchen bezieht sich, wie sich aus Rn. 46 des vorliegenden Urteils ergibt, nur auf die Frage, ob und inwieweit der Zweck der im Ausgangsverfahren in Rede stehenden Regelung geeignet ist, den Zugang öffentlicher Stellen wie der Kriminalpolizei zu solchen Daten zu rechtfertigen, ohne dass die übrigen Zugangsvoraussetzungen nach diesem Art. 15 Abs. 1 Gegenstand dieses Ersuchens wären.

50. Das vorlegende Gericht möchte insbesondere wissen, nach welchen Gesichtspunkten zu beurteilen ist, ob die Straftaten, bezüglich deren den Polizeibehörden zu Ermittlungszwecken der Zugang zu personenbezogenen Daten erlaubt wird, die die Betreiber elektronischer Kommunikationsdienste gespeichert haben, hinreichend schwer sind, um den mit einem solchen Zugang verbundenen Eingriff in die in den Art. 7 und 8 der Charta gewährleisteten Grundrechte, wie sie vom Gerichtshof in seinen Urteilen vom 8. April 2014, *Digital Rights Ireland u. a.* (C-293/12 und C-594/12, EU:C:2014:238), und *Tele2 Sverige und Watson u. a.*, ausgelegt worden sind, zu rechtfertigen.

51. Was das Vorliegen eines Eingriffs in diese Grundrechte betrifft, stellt, wie der Generalanwalt in den Nrn. 76 und 77 seiner Schlussanträge ausgeführt hat, der Zugang der öffentlichen Stellen zu solchen Daten einen Eingriff in das in Art. 7 der Charta verankerte Grundrecht auf Achtung des Privatlebens dar, auch wenn keine Umstände vorliegen, aufgrund deren dieser Eingriff als ‘ schwer ’ eingestuft werden kann, und ohne dass es darauf ankommt, ob die betroffenen Informationen über das Privatleben als sensibel anzusehen sind oder die Betroffenen durch diesen Eingriff irgendwelche Nachteile erlitten haben. Zudem stellt ein solcher Zugang einen Eingriff in das in Art. 8 der Charta garantierte Grundrecht auf Schutz personenbezogener Daten dar, da es sich dabei um eine Verarbeitung personenbezogener Daten handelt (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).

52. Hinsichtlich der Zwecke, die eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende – die den Zugang öffentlicher Stellen zu von Betreibern elektronischer Kommunikationsdienste gespeicherten Daten betrifft und damit vom Grundsatz der Vertraulichkeit elektronischer Kommunikationen abweicht – rechtfertigen können, ist darauf hinzuweisen, dass die Aufzählung der in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 genannten Zwecke abschließend ist, so dass dieser Zugang tatsächlich strikt einem dieser Zwecke dienen muss (vgl. in diesem Sinne Urteil *Tele2 Sverige und Watson u. a.*, Rn. 90 und 115).

53. Was den Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten anbelangt, ist aber festzustellen, dass dieser nach dem Wortlaut von Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 nicht auf die Bekämpfung schwerer Straftaten beschränkt ist, sondern ‘ Straftaten ’ im Allgemeinen betrifft.

54. Insoweit hat der Gerichtshof zwar entschieden, dass im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur die Bekämpfung der schweren

Kriminalität einen Zugang öffentlicher Stellen zu von den Betreibern von Kommunikationsdiensten gespeicherten personenbezogenen Daten rechtfertigen kann, aus deren Gesamtheit genaue Schlüsse auf das Privatleben der von diesen Daten betroffenen Personen gezogen werden können (vgl. in diesem Sinne Urteil *Tele2 Sverige und Watson u. a.*, Rn. 99).

55. Der Gerichtshof hat diese Auslegung jedoch damit begründet, dass der mit einer solchen Zugangsregelung verfolgte Zweck im Verhältnis zur Schwere des damit einhergehenden Eingriffs in die betreffenden Grundrechte stehen muss (vgl. in diesem Sinne Urteil *Tele2 Sverige und Watson u. a.*, Rn. 115).

56. Nach dem Grundsatz der Verhältnismäßigkeit kann ein schwerer Eingriff im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nämlich nur durch einen Zweck der Bekämpfung einer ebenfalls als ‘ schwer ’ einzustufenden Kriminalität gerechtfertigt sein.

57. Ist dagegen der mit einem solchen Zugang verbundene Eingriff nicht schwer, kann dieser Zugang durch einen Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von ‘ Straftaten ’ im Allgemeinen gerechtfertigt sein.

58. Es ist daher zunächst zu prüfen, ob nach den Umständen des vorliegenden Falles der Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte, der mit einem Zugang der Kriminalpolizei zu den im Ausgangsverfahren in Rede stehenden Daten einhergeht, als ‘ schwer ’ anzusehen ist.

59. Insoweit ist festzustellen, dass der im Ausgangsverfahren in Rede stehende Antrag, mit dem die Kriminalpolizei für die Zwecke strafrechtlicher Ermittlungen um gerichtliche Erlaubnis zum Zugang zu von den Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten ersucht, ausschließlich darauf abzielt, die Identität der Inhaber von SIM-Karten festzustellen, die in einem Zeitraum von zwölf Tagen mit der IMEI des gestohlenen Mobiltelefons aktiviert wurden. Wie in Rn. 40 des vorliegenden Urteils ausgeführt, bezieht sich dieser Antrag nur auf den Zugang zu den diesen SIM-Karten entsprechenden Telefonnummern sowie zu den Daten bezüglich der Identität der Karteninhaber wie deren Name, Vorname und gegebenenfalls Adresse. Dagegen beziehen sich diese Daten, wie sowohl die spanische Regierung als auch die Staatsanwaltschaft in der mündlichen Verhandlung bestätigt haben, weder auf die mittels des gestohlenen Mobiltelefons erfolgte Kommunikation noch auf dessen Ortung.

60. Daher kann mit den Daten, auf die sich der im Ausgangsverfahren in Rede stehende Zugangsantrag bezieht, offenbar nur eine Verbindung zwischen der SIM-Karte oder den SIM-Karten, die mit dem gestohlenen Mobiltelefon aktiviert wurden, und der Identität der Inhaber dieser SIM-Karten während eines bestimmten Zeitraums hergestellt werden. Ohne einen Abgleich mit den Daten bezüglich der mittels dieser SIM-Karten erfolgten Kommunikation und den Standortdaten lassen sich diesen Daten weder das Datum, die Uhrzeit, die Dauer und die Adressaten der mittels der betreffenden SIM-Karte bzw. der betreffenden SIM-Karten erfolgten Kommunikation entnehmen noch die Orte, an denen diese Kommunikation erfolgte, oder die Häufigkeit dieser Kommunikation mit bestimmten Personen während eines bestimmten Zeitraums. Aus diesen Daten lassen sich daher keine genauen Schlüsse auf das Privatleben der Personen ziehen, deren Daten betroffen sind.

61. Unter diesen Umständen kann der Zugang nur zu den Daten, auf die sich der im Ausgangsverfahren in Rede stehende Antrag bezieht, nicht als ‘ schwerer ’ Eingriff in die Grundrechte der Personen eingestuft werden, deren Daten betroffen sind.

62. Wie sich aus den Rn. 53 bis 57 des vorliegenden Urteils ergibt, kann der Eingriff, den ein Zugang zu solchen Daten mit sich bringen würde, somit 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, ohne dass es erforderlich wäre, dass diese Straftaten als ‘ schwer ’ einzustufen sind.

63. Nach alledem ist auf die Vorlagefragen zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 der Charta dahin auszulegen ist, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta verankerte Grundreche darstellt, der nicht so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste ».

Im Tenor des Urteils hat der Europäische Gerichtshof für Recht erkannt:

« Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7 und 8 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta der Grundrechte verankerte Grundreche darstellt, der nicht so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste ».

B.13. Mit ihrem Urteil vom 6. Oktober 2020 in der Rechtssache *Privacy International* (C-623/17) hat die Große Kammer des Gerichtshofes entschieden, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht von Artikel 4 Absatz 2 des Vertrags über die Europäische Union sowie der Artikel 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln. Dieses Urteil beruht auf der folgenden Begründung:

« *Zur zweiten Frage*

50. Mit seiner zweiten Frage möchte das vorlegende Gericht wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta und ihres Art. 52 Abs. 1 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln.

51. Zunächst ist darauf hinzuweisen, dass Section 94 des Gesetzes von 1984 nach den Angaben im Vorabentscheidungsersuchen dem Minister gestattet, den Betreibern elektronischer Kommunikationsdienste durch Weisungen vorzuschreiben, den Sicherheits- und Nachrichtendiensten Massen-Kommunikationsdaten, zu denen Verkehrs- und Standortdaten sowie Informationen über die genutzten Dienste im Sinne von Section 21(4) und (6) des RIPA gehören, zu übermitteln, wenn er dies im Interesse der nationalen Sicherheit oder der Beziehungen zu einer ausländischen Regierung für erforderlich hält. Die letztgenannte Bestimmung erfasst u. a. die Daten, die notwendig 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, die IP-Adressen der Quelle und des Adressaten der Kommunikation sowie die Adressen der besuchten Websites.

52. Eine solche Offenlegung durch Übermittlung der Daten betrifft alle Nutzer elektronischer Kommunikationsmittel, ohne dass näher angegeben wird, ob die Übermittlung in Echtzeit oder zeitversetzt erfolgen muss. Im Anschluss an ihre Übermittlung werden diese Daten nach den Angaben im Vorabentscheidungsersuchen von den Sicherheits- und Nachrichtendiensten gespeichert und stehen ihnen für ihre Tätigkeiten ebenso zur Verfügung wie ihre übrigen Datenbanken. Insbesondere können die auf diese Weise gesammelten Daten, die automatisierten Massenverarbeitungen und -analysen unterzogen werden, mit anderen Datenbanken, die andere Kategorien personenbezogener Massendaten enthalten, abgeglichen oder an Stellen außerhalb dieser Dienste und an Drittstaaten weitergegeben werden. Schließlich bedürfen diese Vorgänge keiner vorherigen Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsstelle, und die Betroffenen werden nicht davon unterrichtet.

53. 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 ’.

54. Zu diesem Zweck sieht Art. 5 Abs. 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten ‘ durch innerstaatliche Vorschriften die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten sicher[stellen] ’. Weiter heißt es dort: ‘ Insbesondere untersagen [die Mitgliedstaaten] 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. ’ Art. 5 Abs. 1 ‘ steht – unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen. ’

55. In Art. 5 Abs. 1 der Richtlinie 2002/58 wird somit 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 impliziert, ohne deren Einwilligung solche Nachrichten und Daten auf Vorrat zu speichern. In Anbetracht ihres allgemein gehaltenen Wortlauts gilt diese Bestimmung notwendigerweise für jeden Vorgang, der es Dritten erlaubt, zu anderen Zwecken als der Weiterleitung einer Nachricht Kenntnis von Nachrichten und den damit verbundenen Daten zu erlangen.

56. Das Verbot in Art. 5 Abs. 1 der Richtlinie 2002/58, Nachrichten und die damit verbundenen Daten abzufangen, erfasst deshalb jede Form der Bereitstellung von Verkehrs- und Standortdaten durch die Betreiber elektronischer Kommunikationsdienste für Behörden wie Sicherheits- und Nachrichtendienste sowie die Speicherung solcher Daten durch diese Behörden, unabhängig von einer späteren Verwendung dieser Daten.

57. 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 Daten anonym bleiben und nicht gespeichert werden dürfen, es sei denn, sie haben darin eingewilligt (Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 109).

58. 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.

59. 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 Urteile vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15,

EU:C:2016:970, Rn. 89 und 104, sowie vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 111).

60. 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 die Einhaltung nicht nur 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 Ireland u. a.*, 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).

61. Die gleichen Fragen stellen sich auch für andere Arten der Verarbeitung von Daten, wie ihre Übermittlung an andere Personen als die Nutzer oder den Zugang zu ihnen im Hinblick auf ihre Nutzung (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 122 und 123 sowie die dort angeführte Rechtsprechung).

62. 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 Grundrecht 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).

63. Die in den Art. 7, 8 und 11 der Charta verankerten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden (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).

64. 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.

65. Hinzuzufügen ist, dass das Erfordernis, dass jede Einschränkung der Ausübung von Grundrechten gesetzlich vorgesehen sein muss, bedeutet, dass die gesetzliche Grundlage für den Eingriff in die Grundrechte den Umfang, in dem die Ausübung des betreffenden Rechts

eingeschränkt wird, selbst festlegen muss (Urteil vom 16. Juli 2020, *Facebook Ireland und Schrems*, C-311/18, EU:C:2020:559, Rn. 175 und die dort angeführte Rechtsprechung).

66. 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.

67. 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 Zielsetzung und der fraglichen Rechte und Pflichten 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 Ireland u. a.*, 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).

68. 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 ihrer 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 speziellen Kategorie sensibler personenbezogener Daten geht (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, 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).

69. Zu der Frage, ob eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta den Anforderungen von Art. 15 Abs. 1 der Richtlinie 2002/58 genügt, ist festzustellen, dass die Übermittlung von Verkehrs- und Standortdaten an andere Personen als die Nutzer, etwa an die Sicherheits- und Nachrichtendienste, vom Grundsatz der Vertraulichkeit abweicht. Geschieht dies, wie hier, in allgemeiner und unterschiedsloser Weise, wird die Abweichung von der grundsätzlichen Pflicht zur Gewährleistung der Vertraulichkeit der Daten zur Regel, obwohl das durch die Richtlinie 2002/58 geschaffene System verlangt, dass eine solche Abweichung die Ausnahme bleibt.

70. Zudem stellt nach ständiger Rechtsprechung des Gerichtshofs die Übermittlung von Verkehrs- und Standortdaten an einen Dritten einen Eingriff in die Grundrechte dar, die in den Art. 7 und 8 der Charta verankert sind, unabhängig davon, wie diese Daten später genutzt werden. 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, und Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 115 und 116).

71. Der mit der Übermittlung von Verkehrs- und Standortdaten an die Sicherheits- und Nachrichtendienste verbundene Eingriff in das in Art. 7 der Charta verankerte Recht ist insbesondere angesichts des sensiblen Charakters der Informationen, die diese Daten liefern können, und vor allem angesichts der Möglichkeit, anhand von ihnen ein Profil der Betroffenen zu erstellen, als besonders schwer anzusehen, da eine solche Information ebenso sensibel ist wie der Inhalt der Kommunikationen selbst. Überdies ist er geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist (vgl. entsprechend Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU:C:2014:238, Rn. 27 und 37, sowie vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU:C:2016:970, Rn. 99 und 100).

72. Hinzuzufügen ist, dass eine Übermittlung von Verkehrs- und Standortdaten an Behörden zu Sicherheitszwecken 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 kann. 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 (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU:C:2014:238, Rn. 28, vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU:C:2016:970, Rn. 101, und vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 118).

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

74. Zu den Zielen, die solche Eingriffe rechtfertigen können, und insbesondere zu dem im Ausgangsverfahren in Rede stehenden Ziel der Wahrung der nationalen Sicherheit 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 (Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 135).

75. Die Bedeutung des Ziels, die nationale Sicherheit zu wahren, 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, die nationale Sicherheit zu wahren, daher geeignet, Maßnahmen zu rechtfertigen, die schwerere Grundrechtseingriffe enthalten als solche, die mit den übrigen Zielen gerechtfertigt werden könnten (Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 136).

76. Um dem in Rn. 67 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, die mit einem Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte verbunden ist, jedoch den Anforderungen entsprechen, die sich aus der in den Rn. 65, 67 und 68 des vorliegenden Urteils angeführten Rechtsprechung ergeben.

77. Eine solche Regelung darf sich insbesondere hinsichtlich des Zugangs einer Behörde zu personenbezogenen Daten 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).

78. Infolgedessen, und weil ein allgemeiner Zugang zu allen auf Vorrat gespeicherten Daten ohne jeden - auch nur mittelbaren - Zusammenhang mit dem verfolgten Ziel nicht als auf das absolut Notwendige beschränkt angesehen werden kann, muss sich eine nationale Regelung des Zugangs zu Verkehrs- und Standortdaten bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugang zu den fraglichen Daten zu gewähren ist, auf objektive Kriterien stützen (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).

79. Diese Anforderungen gelten erst recht für eine Rechtsvorschrift wie die im Ausgangsverfahren in Rede stehende, auf deren Grundlage die zuständige nationale Behörde den Betreibern elektronischer Kommunikationsdienste vorschreiben kann, den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten durch eine allgemeine und unterschiedslose Übermittlung offenzulegen. Eine solche Übermittlung hat nämlich zur Folge, dass diese Daten den Behörden zur Verfügung gestellt werden (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 212).

80. Da die Verkehrs- und Standortdaten allgemein und unterschiedslos übermittelt werden, betrifft ihre Übermittlung pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen. 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 Wahrung der nationalen Sicherheit stehen könnte, und setzt insbesondere keinen Zusammenhang zwischen den Daten, deren Übermittlung vorgesehen ist, und einer Bedrohung der nationalen Sicherheit voraus (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, 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). Angesichts dessen, dass die Übermittlung solcher Daten an die Behörden nach den in Rn. 79 des vorliegenden Urteils getroffenen Feststellungen einem Zugang gleichkommt, ist davon auszugehen, dass eine Regelung, die eine allgemeine und unterschiedslose Übermittlung der Daten an die Behörden gestattet, einen allgemeinen Zugang impliziert.

81. Daraus folgt, dass eine nationale Regelung, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten durch eine allgemeine und unterschiedslose Übermittlung offenzulegen, die Grenzen des absolut Notwendigen überschreitet und nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden kann, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta und ihres Art. 52 Abs. 1 verlangt.

82. Nach alledem ist auf die zweite Frage zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta und ihres Art. 52 Abs. 1 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln ».

Im Tenor des Urteils hat der Europäische Gerichtshof für Recht erkannt:

« 2. Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union und ihres Art. 52 Abs. 1 dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln ».

B.14. Mit ihrem Urteil *La Quadrature du Net und andere* (C-511/18, C-512/18 und C-520/18) vom 6. Oktober 2020 hat die Große Kammer des Gerichtshofes der Europäischen Union die ersten zwei vom Gerichtshof mit seinem Entscheid Nr. 96/2018 gestellten Fragen wie folgt beantwortet:

« 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.

[...]

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 ».

Im Tenor des Urteils hat der Europäische Gerichtshof 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.

[…] ».

B.15. Aus dem vorerwähnten Urteil des Gerichtshofes in der Rechtssache *La Quadrature du Net und andere* vom 6. Oktober 2020 geht hervor, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7, 8 und 11 sowie von Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen ist, dass er Rechtsvorschriften entgegensteht, die zu den in Artikel 15 Absatz 1 genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und

Standortdaten vorsehen, außer in den von dem vorerwähnten Urteil beschriebenen begrenzten Fällen.

Insofern es grundsätzlich und ohne Begrenzung auf diese Fälle eine allgemeine und unterschiedslose Vorratsspeicherung von Identifizierungs-, Zugangs- und Verbindungsdaten sowie der in Artikel 126 § 3 des Gesetzes vom 13. Juni 2005 erwähnten Kommunikationsdaten durch die Betreiber und Anbieter von elektronischen Kommunikationsdiensten vorsieht, verstößt das angefochtene Gesetz folglich gegen Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Lichte der vorerwähnten Bestimmungen der Charta der Grundrechte der Europäischen Union und in Verbindung mit den Artikeln 10 und 11 der Verfassung.

B.16.1. Im Tenor des vorerwähnten Urteils in der Rechtssache *La Quadrature du Net und andere* vom 6. Oktober 2020 hat der Gerichtshof der Europäischen Union jedoch präzisiert, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7, 8 und 11 sowie von Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union verschiedenen Arten von Rechtsvorschriften nicht entgegensteht, die darin aufgezählt sind. So sind unter anderem Rechtsvorschriften zulässig, die « 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 » oder auch Rechtsvorschriften, die « 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 ». 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 ».

B.16.2. Auf der Grundlage dieser Präzisierungen des Gerichtshofes der Europäischen Union führt der Ministerrat in seinen Ergänzungsschriftsätzen an, dass das angefochtene Gesetz in jedem Fall nicht für nichtig zu erklären sei, insofern es die allgemeine und unterschiedslose Pflicht zur Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, einerseits und der die Identität der Nutzer elektronischer Kommunikationsmittel

betreffenden Daten andererseits durch die Betreiber und Anbieter von elektronischen Kommunikationsdiensten vorsehe.

Der Ministerrat zieht daraus den Schluss, dass gegebenenfalls nur die Absätze 2 und 3 von Artikel 126 § 3 des Gesetzes vom 13. Juni 2005, die jeweils die Verbindungs- und Standortdaten und die Kommunikationsdaten betreffen, für nichtig zu erklären seien. Er ist der Auffassung, dass Absatz 1 des vorerwähnten Artikels 126 § 3, der sich auf die Identifizierungsdaten bezieht, hingegen nicht für nichtig erklärt werden muss, ebenso wenig wie die anderen Bestimmungen des angefochtenen Gesetzes, da sie die notwendigen Garantien hinsichtlich der Vorratsspeicherung der Daten und des Zugangs zu ihnen enthielten.

B.17. Im vorliegenden Fall ist festzustellen, dass das angefochtene Gesetz im Grundsatz auf einer allgemeinen und unterschiedslosen Vorratsspeicherungspflicht für sämtliche in Artikel 126 § 3 des Gesetzes vom 13. Juni 2005 erwähnten Daten beruht und dass es allgemein, wie in B.3 und B.4 erwähnt, umfassendere Ziele als die Bekämpfung schwerer Kriminalität oder die Gefahr einer schwerwiegenden Beeinträchtigung der öffentlichen Sicherheit verfolgt.

Die Unterscheidung, die in Artikel 126 § 3 des Gesetzes vom 13. Juni 2005 zwischen drei Datenkategorien (nämlich den Identifizierungsdaten, den Zugangs- und Verbindungsdaten sowie den Kommunikationsdaten) vorgenommen wird, wirkt sich nur auf den Anfangszeitpunkt der Dauer der Datenspeicherung von in jedem Fall zwölf Monaten und eventuell auf die Möglichkeiten, auf sie zuzugreifen, für die ermächtigten Stellen aus (siehe Artikel 46*bis* des Strafprozessgesetzbuches und Artikel 126 § 2 des Gesetzes vom 13. Juni 2005). Diese Kategorisierung entspricht außerdem nicht den Unterscheidungen, die vom Gerichtshof der Europäischen Union in seinem Urteil vom 6. Oktober 2020 in Bezug auf die verschiedenen Datenkategorien, die Gegenstand einer allgemeinen und unterschiedslosen Vorratsspeicherungspflicht unter Einhaltung mehrere Bedingungen sein können (nämlich im vorliegenden Fall: die IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, und die Daten, die die Identität der Nutzer elektronischer Kommunikationsmittel betreffen), vorgenommen werden.

B.18. Das Urteil des Gerichtshofes vom 6. Oktober 2020 verpflichtet zu einer Änderung der Perspektive hinsichtlich der Entscheidung des Gesetzgebers: Die Pflicht zur Speicherung von Daten über die elektronische Kommunikation muss die Ausnahme sein und nicht die Regel.

Eine Regelung, die eine solche Pflicht vorsieht, muss zudem klaren und präzisen Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme unterliegen und Mindesterfordernisse aufstellen (Randnr. 133). Diese Regelung muss gewährleisten, dass sich der Eingriff auf das absolut Notwendige beschränkt und muss stets « objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen » (Randnrn. 132 und 133).

B.19. Es obliegt dem Gesetzgeber, eine Regelung auszuarbeiten, mit der die auf dem Gebiet des Schutzes personenbezogener Daten geltenden Grundsätze im Lichte der Rechtsprechung des Gerichtshofes der Europäischen Union eingehalten werden, und gegebenenfalls die von diesem angegebenen Präzisierungen in Bezug auf die verschiedenen Arten von Rechtsvorschriften, die als vereinbar mit Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Lichte der Artikel 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union betrachtet werden, zu berücksichtigen. Insbesondere obliegt es ebenfalls dem Gesetzgeber, in diesem Kontext die Unterscheidungen vorzunehmen, die zwischen den verschiedenen der Vorratsspeicherung unterliegenden Datenarten notwendig sind, sodass gewährleistet ist, dass sich der Eingriff für jede Datenart auf das absolut Notwendige beschränkt.

B.20. In Anbetracht des Vorstehenden sind die Artikel 2 Buchstabe b), 3 bis 11 und 14 des angefochtenen Gesetzes, die untrennbar miteinander verbunden sind, für nichtig zu erklären.

B.21. Die anderen Klagegründe in den Rechtssachen Nrn. 6599 und 6601 betreffen ebenfalls die allgemeine und unterschiedslose Vorratsspeicherung von Daten über die elektronische Kommunikation und den Zugang zu ihnen. Da sie nicht zu einer weitergehenden Nichtigerklärung führen können, erübrigt sich ihre Prüfung.

In Bezug auf die Aufrechterhaltung der Folgen

B.22. In seinen Gegenerwiderungsschriftsätzen beantragt der Ministerrat äußerst hilfsweise, die Folgen der Bestimmungen, die gegebenenfalls für nichtig erklärt würden, aufrechtzuerhalten, um die Arbeit zur Ermittlung und Verfolgung von Straftaten der Polizei- und Nachrichtendienste nicht zu gefährden.

B.23.1. Artikel 8 Absatz 3 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof bestimmt:

« Wenn der Verfassungsgerichtshof es für notwendig erachtet, gibt er im Wege einer allgemeinen Verfügung die Folgen der für nichtig erklärten Bestimmungen an, die als endgültig zu betrachten sind oder für die von ihm festgelegte Frist vorläufig aufrechterhalten werden ».

B.23.2. Der Gerichtshof muss diesbezüglich die Einschränkungen berücksichtigen, die sich aus dem Recht der Europäischen Union bezüglich der Aufrechterhaltung der Folgen innerstaatlicher Normen, die für nichtig zu erklären sind, weil sie im Widerspruch zu diesem Recht stehen, ergeben (EuGH, Große Kammer, 8. September 2010, C-409/06, *Winner Wetten*, Randnrn. 53-69; EuGH, Große Kammer, 28. Februar 2012, C-41/11, *Inter-Environnement Wallonie und Terre wallonne*, Randnrn. 56-63).

In der Regel kann diese Aufrechterhaltung der Folgen nur unter den Bedingungen geschehen, die durch den Europäischen Gerichtshof in der Antwort auf eine Vorabentscheidungsfrage festgelegt werden.

B.24.1. In Beantwortung der dritten vom Gerichtshof gestellten Vorabentscheidungsfrage zu einer etwaigen Aufrechterhaltung der Folgen des angefochtenen Gesetzes hat der Gerichtshof der Europäischen Union geurteilt:

« *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 ».

Im Tenor des Urteils hat der Europäische Gerichtshof für Recht erkannt:

« 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 ».

B.24.2. Aus dem vorerwähnten Urteil geht hervor, dass der Gerichtshof die Folgen der für nichtig erklärten Bestimmungen nicht vorläufig aufrechterhalten darf.

B.24.3. Es obliegt dem zuständigen Strafrichter, gegebenenfalls gemäß Artikel 32 des einleitenden Titels des Strafprozessgesetzbuches und im Lichte der vom Gerichtshof der Europäischen Union im vorerwähnten Urteil vom 6. Oktober 2020 angegebenen Präzisierungen über die Zulässigkeit von Beweisen zu befinden, die bei der Umsetzung der für nichtig erklärten Bestimmungen gesammelt wurden.

Aus diesen Gründen:

Der Gerichtshof

erklärt die Artikel 2 Buchstabe *b)*, 3 bis 11 und 14 des Gesetzes vom 29. Mai 2016 « über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation » für nichtig und weist die Klagen im Übrigen zurück.

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 22. April 2021.

Der Kanzler, Der Präsident,

F. Meersschaut F. Daoût