Geschäftsverzeichnisnr. 6672
Entscheid Nr. 158/2021 vom 18. November 2021

E N T S C H E I D

In Sachen: Klage auf Nichtigerklärung des Gesetzes vom 1. September 2016 « zur Abänderung von Artikel 127 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation und von Artikel 16/2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste », erhoben von Patrick Van Assche und anderen.

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten L. Lavrysen und P. Nihoul, den Richtern J.-P. Moerman, T. Giet, R. Leysen, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne und D. Pieters, und dem emeritierten Präsidenten F. Daoût und der emeritierten Richterin T. Merckx-Van Goey gemäß Artikel 60*bis* des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, unter Assistenz des Kanzlers P.-Y. Dutilleux, unter dem Vorsitz des Präsidenten L. Lavrysen,

erlässt nach Beratung folgenden Entscheid:

*

* *

I. *Gegenstand der Klage und Verfahren*

Mit einer Klageschrift, die dem Gerichtshof mit am 7. Juni 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 8. Juni 2017 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung des Gesetzes vom 1. September 2016 « zur Abänderung von Artikel 127 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation und von Artikel 16/2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste » (veröffentlicht im *Belgischen Staatsblatt* vom 7. Dezember 2016): Patrick Van Assche, Christel Van Akeleyen und Karina De Hoog, unterstützt und vertreten durch RA D. Pattyn, in Westflandern zugelassen.

Der Ministerrat, unterstützt und vertreten durch RA S. Depré, RA E. de Lophem und RÄin T. Wouters, in Brüssel zugelassen, hat einen Schriftsatz eingereicht, die klagenden Parteien haben einen Erwiderungsschriftsatz eingereicht, und der Ministerrat hat auch einen Gegenerwiderungsschriftsatz eingereicht.

Durch Anordnung vom 7. Februar 2018 hat der Gerichtshof nach Anhörung der referierenden Richter A. Alen und J.-P. Moerman beschlossen, dass die Rechtssache verhandlungsreif ist, 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 28. Februar 2018 geschlossen und die Rechtssache zur Beratung gestellt wird.

Infolge des Antrags der klagenden Parteien auf Anhörung hat der Gerichtshof durch Anordnung vom 1. März 2018 den Sitzungstermin auf den 21. März 2018 anberaumt.

Durch Anordnung vom 28. März 2018 hat der Gerichtshof die Rechtssache auf die Sitzung vom 25. April 2018 vertagt.

Auf der öffentlichen Sitzung vom 25. April 2018

- erschienen

. RA D. Pattyn, für die klagenden Parteien, und Patrick Van Assche, persönlich,

. RA. E. de Lophem, RÄin T. Wouters und RA G. Ryelandt, in Brüssel zugelassen, *loco* RA S. Depré, für den Ministerrat,

- haben der Präsident A. Alen und der Richter J.-P. Moerman Bericht erstattet,

- wurden die vorgenannten Parteien angehört,

- wurde die Rechtssache zur Beratung gestellt.

Durch Anordnung vom 19. Juli 2018 hat der Gerichtshof die Behandlung der Rechtssache auf unbestimmte Zeit ausgesetzt.

Durch Anordnung vom 21. April 2021 hat der Gerichtshof nach Anhörung der referierenden Richter D. Pieters, in Vertretung des emeritierten Präsidenten A. Alen, und T. Giet, in Vertretung des gesetzlich verhinderten Richters J.-P. Moerman, beschlossen,

- die Verhandlung wiederzueröffnen,

- die Parteien aufzufordern, in einem spätestens am 31. Mai 2021 einzureichenden und innerhalb derselben Frist den jeweils anderen Parteien in Kopie zu übermittelnden Ergänzungsschriftsatz ihren Standpunkt zu den Auswirkungen des Urteils des Gerichtshofes der Europäischen Union vom 6. Oktober 2020 in den Rechtssachen Nrn. C-511/18, C-512/18 und C-520/18 und des Entscheids des Verfassungsgerichtshofes Nr. 57/2021 vom 22. April 2021 auf die vorliegende Nichtigkeitsklage zu äußern,

- 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,

- dass im Falle eines solchen Antrags die Rechtssache auf der Sitzung vom 16. Juni 2021 zu der später vom Präsidenten zu bestimmenden Uhrzeit behandelt wird, und

- dass vorbehaltlich eines solchen Antrags die Verhandlung am 16. Juni 2021 geschlossen und die Rechtssache zur Beratung gestellt wird.

Ergänzungsschriftsätze wurden eingereicht von

- den klagenden Parteien,

- dem Ministerrat, unterstützt und vertreten durch RA S. Depré, RA E. de Lophem und RA G. Ryelandt.

Infolge des Antrags des Ministerrates auf Anhörung hat der Präsident durch Anordnung vom 5. Mai 2021 die Uhrzeit des Sitzungstermins vom 16. Juni 2021 auf 14.00 Uhr festgelegt.

Auf der öffentlichen Sitzung vom 16. Juni 2021

- erschienen

. RA D. Pattyn, für die klagenden Parteien, und Patrick Van Assche, persönlich,

. RA. E. de Lophem und RA G. Ryelandt, ebenfalls *loco* RA S. Depré, für den Ministerrat,

- haben die referierenden Richter D. Pieters und J.-P. Moerman Bericht erstattet,

- wurden die vorgenannten Parteien angehört,

- wurde die Rechtssache 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*

(…)

B.1.1. Das Gesetz vom 1. September 2016 « zur Abänderung von Artikel 127 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation und von Artikel 16/2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste » (nachstehend: angefochtenes Gesetz) bestimmt:

« KAPITEL 1. - *Gegenstand*

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 127 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation, abgeändert durch die Gesetze vom 4. Februar 2010, 10. Juli 2012, 27. März 2014 und 29. Mai 2016, wird wie folgt abgeändert:

1. Paragraph 1 wird wie folgt abgeändert:

a) In Absatz 1 werden zwischen den Wörtern ‘ wie in Artikel 126 § 1 Absatz 1 erwähnt ’ und den Wörtern ‘ und Endnutzern ’ die Wörter ‘ , Vertriebswegen elektronischer Kommunikationsdienste, Unternehmen, die einen Identifizierungsdienst bereitstellen, ’ eingefügt.

b) [Abänderung des niederländischen Textes]

c) Zwischen Absatz 1 und Absatz 2 werden sieben Absätze mit folgendem Wortlaut eingefügt:

‘ Was die Identifizierung des Endnutzers betrifft, ist der Betreiber oder Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt der für die Verarbeitung Verantwortliche im Sinne des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten.

Außer bei Beweis des Gegenteils gilt die identifizierte Person als Nutzer des elektronischen Kommunikationsdienstes.

Wenn der Endnutzer ein Identifizierungsdokument mit der Nationalregisternummer vorlegt, sammelt der Betreiber, der Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt, der

Vertriebsweg elektronischer Kommunikationsdienste oder das Unternehmen, das einen Identifizierungsdienst bereitstellt, diese Nummer.

Der Vertriebsweg elektronischer Kommunikationsdienste speichert keine Identifizierungsdaten oder -dokumente auf Vorrat, die dem Betreiber, dem Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt oder dem Unternehmen, das einen Identifizierungsdienst bereitstellt, übermittelt werden.

Wenn eine direkte Eingabe in die Datenverarbeitungssysteme des Betreibers, des Anbieters wie in Artikel 126 § 1 Absatz 1 erwähnt oder des Unternehmens, das einen Identifizierungsdienst bereitstellt, nicht möglich ist, darf der Vertriebsweg elektronischer Kommunikationsdienste eine Kopie des Identifizierungsdokuments machen, unter anderem des belgischen elektronischen Personalausweises; diese Kopie wird jedoch spätestens nach Aktivierung des elektronischen Kommunikationsdienstes vernichtet.

Betreiber oder Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt bewahren eine Kopie anderer Identifizierungsdokumente als den belgischen elektronischen Personalausweis.

Die gesammelten Identifizierungsdaten und -dokumente werden gemäß Artikel 126 § 3 Absatz 1 auf Vorrat gespeichert. ’

2. Paragraph 3 wird durch einen Absatz mit folgendem Wortlaut ergänzt:

‘ Nicht identifizierte Endnutzer - wie durch den in § 1 erwähnten Königlichen Erlass bestimmt - von Guthabenkarten, die vor Inkrafttreten des in § 1 erwähnten Königlichen Erlasses gekauft worden sind, identifizieren sich binnen der von Betreiber oder Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt festgelegten Frist; diese Frist darf sechs Monate nach Veröffentlichung des in § 1 erwähnten Königlichen Erlasses nicht überschreiten. Das in § 2 erwähnte Verbot findet erst Anwendung nach Ablauf der Frist, die dem Endnutzer im Hinblick auf seine Identifizierung gewährt wird. ’

3. Paragraph 4 wird wie folgt abgeändert:

a) Zwischen dem Wort ‘ Betreiber ’ und den Wörtern ‘ ihnen auferlegte technische und administrative Maßnahmen ’ werden die Wörter ‘ oder Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt ’ eingefügt.

b) [Abänderung des niederländischen Textes]

c) [Abänderung des niederländischen Textes]

d) Die Wörter ‘ Setzen Betreiber ihnen auferlegte technische und administrative Maßnahmen nicht innerhalb der vom König festgelegten Frist um ’ werden durch die Wörter ‘ Setzen Betreiber ihnen durch vorliegenden Artikel oder vom König auferlegte technische und administrative Maßnahmen nicht um ’ ersetzt.

e) [Abänderung des niederländischen Textes]

4. Paragraph 5 wird wie folgt abgeändert:

a) In Absatz 1 werden zwischen dem Wort ‘ Betreiber ’ und den Wörtern ‘ trennen Endnutzer ’ die Wörter ‘ und Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt ’ eingefügt.

b) *Abänderung des niederländischen Textes]*

c) Die Wörter ‘ die ihnen auferlegte technische und administrative Maßnahmen nicht innerhalb der vom König festgelegten Frist umgesetzt haben ’ werden durch die Wörter ‘ die ihnen durch vorliegenden Artikel oder vom König auferlegte technische und administrative Maßnahmen nicht umgesetzt haben ’ ersetzt.

d) [Abänderung des niederländischen Textes]

e) [Abänderung des niederländischen Textes];

f) Absatz 2 wird aufgehoben.

KAPITEL 3. - *Abänderungen des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste*

Art. 3. Artikel 16/2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste, eingefügt durch das Gesetz vom 5. Februar 2016, wird wie folgt abgeändert:

1. Die heutigen Absätze 1 bis 4 werden § 1 bilden und im französischen Text wird das Wort ‘ chef ’ jeweils durch das Wort ‘ dirigeant ’ ersetzt.

2. Ein Paragraph 2 mit folgendem Wortlaut wird eingefügt:

‘ § 2. Die Nachrichten- und Sicherheitsdienste können im Interesse der Erfüllung ihrer Aufträge die Mitwirkung einer Bank oder eines Finanzinstituts anfordern, um die Identifizierung des Endnutzers einer in Artikel 127 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation erwähnten Guthabenkarte auf der Grundlage der Bezugsnummer eines elektronischen Bankgeschäfts vorzunehmen, das sich auf diese Guthabenkarte bezieht und vorher in Anwendung von § 1 von einem Betreiber oder einem Anbieter mitgeteilt worden ist.

Die Anforderung erfolgt schriftlich durch den Dienstleiter oder seinen Beauftragten. Bei äußerster Dringlichkeit kann der Dienstleiter beziehungsweise sein Beauftragter diese Daten mündlich anfordern. Diese mündliche Anforderung wird binnen vierundzwanzig Stunden durch eine schriftliche Anforderung bestätigt.

Jede Bank und jedes Finanzinstitut, dessen Mitwirkung angefordert wird, verschafft dem Dienstleiter beziehungsweise seinem Beauftragten unverzüglich die angeforderten Daten.

Die Identifizierungsdaten, die die Nachrichten- und Sicherheitsdienste im Rahmen der im vorliegenden Paragraphen erwähnten Vorgehensweise erhalten, sind auf die in § 1 erwähnten Identifizierungsdaten begrenzt. ’

3. Der heutige Absatz 5 wird § 3 bilden.

4. Im heutigen Absatz 6, dessen Wortlaut § 4 bilden wird, werden die Wörter ‘ den betreffenden Nachrichten- und Sicherheitsdiensten ’ durch die Wörter ‘ dem betreffenden Nachrichten- und Sicherheitsdienst ’ ersetzt ».

B.1.2. Das angefochtene Gesetz ist Bestandteil der Antiterrormaßnahmen, die im Anschluss an die Terroranschläge vom 13. November 2015 in Paris und vom 22. März 2016 in Brüssel getroffen worden sind (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1964/001, S. 2). Artikel 2 des angefochtenen Gesetzes ändert Artikel 127 des Gesetzes vom 13. Juni 2005 « über die elektronische Kommunikation » (nachstehend: Gesetz vom 13. Juni 2005) im Hinblick auf die Abschaffung der Anonymität bei Guthabenkarten ab. Artikel 3 des angefochtenen Gesetzes ändert Artikel 16/2 des Grundlagengesetzes vom 30. November 1998 « über die Nachrichten- und Sicherheitsdienste » (nachstehend: Gesetz vom 30. November 1998) ab, um die Identifizierung des Endnutzers einer Guthabenkarte auf der Grundlage des Online-Bankgeschäfts, über das sie gekauft wurde, zu ermöglichen.

B.2.1. Der durch Artikel 2 des angefochtenen Gesetzes abgeänderte Artikel 127 des Gesetzes vom 13. Juni 2005 bestimmt:

« § 1. Der König legt nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts technische und administrative Maßnahmen fest, die Betreibern, Anbietern wie in Artikel 126 § 1 Absatz 1 erwähnt, Vertriebswegen elektronischer Kommunikationsdienste, Unternehmen, die einen Identifizierungsdienst bereitstellen, und Endnutzern auferlegt werden, um Folgendes zu ermöglichen:

1. Identifizierung des Anrufers im Rahmen eines Notrufs,

2. Identifizierung des Endnutzers und Ermittlung, Lokalisierung, Mithören, Kenntnisnahme und Aufzeichnung privater Nachrichten unter den in den Artikeln 46*bis*, 88*bis* und 90*ter* bis 90*decies* des Strafprozessgesetzbuchs und den im Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste vorgesehenen Bedingungen.

Was die Identifizierung des Endnutzers betrifft, ist der Betreiber oder Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt der für die Verarbeitung Verantwortliche im Sinne des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten.

Außer bei Beweis des Gegenteils gilt die identifizierte Person als Nutzer des elektronischen Kommunikationsdienstes.

Wenn der Endnutzer ein Identifizierungsdokument mit der Nationalregisternummer vorlegt, sammelt der Betreiber, der Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt, der Vertriebsweg elektronischer Kommunikationsdienste oder das Unternehmen, das einen Identifizierungsdienst bereitstellt, diese Nummer.

Der Vertriebsweg elektronischer Kommunikationsdienste speichert keine Identifizierungsdaten oder -dokumente auf Vorrat, die dem Betreiber, dem Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt oder dem Unternehmen, das einen Identifizierungsdienst bereitstellt, übermittelt werden.

Wenn eine direkte Eingabe in die Datenverarbeitungssysteme des Betreibers, des Anbieters wie in Artikel 126 § 1 Absatz 1 erwähnt oder des Unternehmens, das einen Identifizierungsdienst bereitstellt, nicht möglich ist, darf der Vertriebsweg elektronischer Kommunikationsdienste eine Kopie des Identifizierungsdokuments machen, unter anderem des belgischen elektronischen Personalausweises; diese Kopie wird jedoch spätestens nach Aktivierung des elektronischen Kommunikationsdienstes vernichtet.

Betreiber oder Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt bewahren eine Kopie anderer Identifizierungsdokumente als den belgischen elektronischen Personalausweis.

Die gesammelten Identifizierungsdaten und -dokumente werden gemäß Artikel 126 § 3 Absatz 1 auf Vorrat gespeichert..

Der König legt nach Stellungnahme des Instituts die Tarife zur Vergütung der Beteiligung der Betreiber und Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt an den in Absatz 1 Nr. 2 erwähnten Handlungen fest, und die Frist für die Umsetzung der auferlegten Maßnahmen durch Betreiber beziehungsweise Teilnehmer.

§ 2. Bereitstellung oder Nutzung von Diensten oder Ausrüstungen, die die in § 1 erwähnten Handlungen erschweren oder unmöglich machen, mit Ausnahme von Verschlüsselungssystemen, die Vertraulichkeit der Kommunikation und Zahlungssicherheit gewährleisten können, sind verboten.

§ 3. Bis zum Inkrafttreten der in § 1 erwähnten Maßnahmen ist das in § 2 vorgesehene Verbot nicht auf öffentlich zugängliche elektronische Mobilfunkdienste anwendbar, die über eine Guthabenkarte abgerechnet werden.

Nicht identifizierte Endnutzer - wie durch den in § 1 erwähnten Königlichen Erlass bestimmt - von Guthabenkarten, die vor Inkrafttreten des in § 1 erwähnten Königlichen Erlasses gekauft worden sind, identifizieren sich binnen der von Betreiber oder Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt festgelegten Frist; diese Frist darf sechs Monate nach Veröffentlichung des in § 1 erwähnten Königlichen Erlasses nicht überschreiten. Das in § 2 erwähnte Verbot findet erst Anwendung nach Ablauf der Frist, die dem Endnutzer im Hinblick auf seine Identifizierung gewährt wird.

§ 4. Setzen Betreiber oder Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt ihnen durch vorliegenden Artikel oder vom König auferlegte technische und administrative Maßnahmen nicht um, so dürfen sie Dienste, für die die betreffenden Maßnahmen nicht ergriffen worden sind, nicht mehr bereitstellen.

§ 5. Betreiber und Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt trennen Endnutzer, die ihnen durch vorliegenden Artikel oder vom König auferlegte technische und administrative Maßnahmen nicht umgesetzt haben, von Netzen und Diensten ab, auf die die auferlegten

Maßnahmen anwendbar sind. Diese Endnutzer werden auf keinerlei Weise für diese Abtrennung entschädigt ».

B.2.2. Artikel 127 des Gesetzes vom 13. Juni 2005 lag immer das Prinzip zugrunde, dass alle Endnutzer elektronischer Kommunikationsnetzwerke identifizierbar sein müssen. Ursprünglich sah diese Bestimmungen nur Verpflichtungen für die Betreiber, die Anbieter und die Endnutzer dieser Dienste vor. Artikel 127 § 1 Absatz 1 enthält eine allgemeine Ermächtigung zugunsten des Königs, die technischen und administrativen Maßnahmen festzulegen, um diese Identifizierbarkeit zu ermöglichen.

Diese Identifizierbarkeit dient zwei Zielen. Erstens soll sie das gute Funktionieren der Notdienste unterstützen, indem sie ermöglicht, dass der Anrufer im Rahmen eines Notrufs identifiziert wird (Artikel 127 § 1 Absatz 1 Nr. 1). Zweitens trägt sie dazu bei, private Nachrichten unter den in den Artikeln 46*bis*, 88*bis* und 90*ter* bis 90*decies* des Strafprozessgesetzbuches und den im Gesetz vom 30. November 1998 vorgesehenen Bedingungen zu ermitteln, zu lokalisieren, abzuhören, zur Kenntnis zu nehmen und aufzuzeichnen (Artikel 127 § 1 Absatz 1 Nr. 2).

Artikel 127 § 2 des Gesetzes vom 13. Juni 2005 verbietet die Bereitstellung oder die Nutzung von Diensten oder Ausrüstungen, die die Identifizierbarkeit erschweren, mit Ausnahme von Verschlüsselungssystemen, die die Vertraulichkeit der Kommunikation und die Zahlungssicherheit gewährleisten können.

Artikel 127 § 3 desselben Gesetzes sah ursprünglich eine zeitlich befristete Ausnahme von diesem Verbot für die Endnutzer von Guthabenkarten vor. Diese Endnutzer waren vom Erfordernis der Identifizierbarkeit befreit, solange der König die in Artikel 127 § 1 genannten technischen und administrativen Maßnahmen noch nicht festgelegt hatte.

B.2.3. Artikel 2 des angefochtenen Gesetzes hat Artikel 127 des Gesetzes vom 13. Juni 2005 an verschiedenen Stellen abgeändert. Erstens hat er seinen Anwendungsbereich erweitert, indem er einige der darin geregelten Verpflichtungen auch den Vertriebswegen elektronischer Kommunikationsdienste und den Unternehmen, die einen Identifizierungsdienst bereitstellen, auferlegt hat.

Zweitens hat diese Bestimmung einige Aspekte der Identifizierung des Endnutzers gesetzlich verankert. So werden der Betreiber und der Anbieter zu Verarbeitern in Bezug auf personenbezogene Daten bestimmt (Artikel 127 § 1 Absatz 2). Ebenso wird festgelegt, dass vorbehaltlich des Beweises des Gegenteils die identifizierte Person als Nutzer des elektronischen Kommunikationsdienstes gilt (Artikel 127 § 1 Absatz 3), dass die Identifizierung anhand eines Identifizierungsdokuments mit der Nationalregisternummer erfolgen muss (Artikel 127 § 1 Absatz 4) und dass der Vertriebsweg elektronischer Kommunikationsdienste keine Kopien der Identifizierungsdaten oder -dokumente, die dem Betreiber übermittelt werden, auf Vorrat speichern darf (Artikel 127 § 1 Absätze 5 bis 7).

Drittens enthält diese Bestimmung einige spezifische Ermächtigungen zugunsten des Königs wie die Ermächtigung im neuen Artikel 127 § 1 Absatz 8 des Gesetzes vom 13. Juni 2005, die Vergütung der Betreiber und Anbieter für die Fälle festzulegen, in denen sie an der Identifizierung der Endnutzer ihrer Dienste mitwirken müssen, und die Frist für die Umsetzung der auferlegten Maßnahmen durch Betreiber beziehungsweise Teilnehmer. Der neue zweite Absatz von Artikel 127 § 3 des Gesetzes vom 13. Juni 2005 ermächtigt den König, die Frist zu bestimmen, innerhalb deren sich der Endnutzer einer Guthabenkarte, die vor Inkrafttreten des angefochtenen Gesetzes gekauft wurde, identifizieren muss. Diese Frist darf sechs Monate nach Veröffentlichung des in Artikel 127 § 1 desselben Gesetzes erwähnten königlichen Erlasses nicht überschreiten. Nach dem neuen Artikel 127 § 3 Absatz 2 des Gesetzes vom 13. Juni 2005 gilt die Anonymität bei Guthabenkarten erst nach Ablauf dieser Frist als aufgehoben.

B.2.4. Der König hat Artikel 127 des Gesetzes vom 13. Juni 2005, jedenfalls in Bezug auf die elektronischen Kommunikationsdienste, die auf der Grundlage einer Guthabenkarte angeboten werden, durch den königlichen Erlass vom 27. November 2016 « über die Identifizierung des Endnutzers öffentlich zugänglicher elektronischer Mobilfunkdienste, die über eine Guthabenkarte abgerechnet werden » (nachstehend: königlicher Erlass vom 27. November 2016) umgesetzt.

Artikel 2 Nr. 4 des königlichen Erlasses definiert ein gültiges Identifizierungsdokument als « den belgischen Personalausweis oder den Personalausweis eines Mitgliedstaates der Europäischen Union, die belgische elektronische Ausländerkarte, das Dokument mit der Nummer, die in Artikel 8 § 1 Nr. 2 des Gesetzes vom 15. Januar 1990 über die Errichtung und Organisation einer Zentralen Datenbank der sozialen Sicherheit oder in Artikel 2 Absatz 2 des

Gesetzes vom 8. August 1983 zur Organisation eines Nationalregisters der natürlichen Personen erwähnt ist, oder den internationalen Reisepass oder das offizielle Dokument zur zeitweiligen Ersetzung eines der vorerwähnten Dokumente, das verloren gegangen ist oder gestohlen wurde, sofern es sich bei dem Identifizierungsdokument um ein lesbares und gültiges Original handelt ».

Die Artikel 3 bis 6 des königlichen Erlasses vom 27. November 2016 sehen Verpflichtungen für die Endnutzer von Guthabenkarten vor. Sie müssen sich selbst beim Betreiber jedes Mal identifizieren, wenn er dies verlangt. Wenn sie eine neue Guthabenkarte kaufen, teilen sie ihre Identität dem Betreiber spätestens bei Aktivierung der Karte nach einer gültigen Identifizierungsmethode mit. Es ist ihnen grundsätzlich untersagt, ihre Guthabenkarte Dritten zu überlassen, außer in den in Artikel 5 des königlichen Erlasses geregelten Fällen und unter den dort geregelten Bedingungen. Wenn sie ihre Guthabenkarte verlieren oder wenn diese gestohlen wird, müssen sie den Betreiber davon binnen vierundzwanzig Stunden in Kenntnis setzen.

Die Artikel 7 bis 9 desselben königlichen Erlasses sehen Verpflichtungen für Betreiber vor. Sie mussten alle Endnutzer von Guthabenkarten, die vor Inkrafttreten dieses königlichen Erlasses am 17. Dezember 2016 verkauft wurden, vor dem 7. Juni 2017 identifizieren. Seit Inkrafttreten dieses königlichen Erlasses dürfen sie keine neuen Guthabenkarten aktivieren, wenn der Endnutzer noch nicht identifiziert ist. Wenn der Endnutzer sie vom Verlust oder Diebstahl der Guthabenkarte in Kenntnis setzt, müssen sie diese sofort unbrauchbar machen.

B.2.5. Die Artikel 9 bis 12 desselben königlichen Erlasses bestimmen, wie der Endnutzer einer Guthabenkarte zu identifizieren ist und wie seine Identifizierungsdaten verarbeitet werden. Betreiber, Identifizierungsdiensteanbieter oder Vertriebswege elektronischer Kommunikationsdienste sammeln diese Daten, indem sie den belgischen elektronischen Personalausweis elektronisch lesen oder ihn einschließlich des darauf abgebildeten Fotos und seiner Nummer einscannen, kopieren oder fotografieren. Der Betreiber muss vor Aktivierung der Guthabenkarte überprüfen, ob der vorgelegte Personalausweis gestohlen oder zu betrügerischen Zwecken verwendet wurde.

Der Betreiber speichert die zur Identifizierung des Endnutzers verwendete Identifizierungsmethode, solange die Identifizierungsdaten des Endnutzers aufgrund von

Artikel 126 des Gesetzes vom 13. Juni 2005 auf Vorrat gespeichert werden können. Die vom Betreiber auf Vorrat zu speichernden Daten hängen von der ausgewählten Identifizierungsmethode ab, umfassen aber höchstens Namen und Vornamen, Geschlecht, Staatsangehörigkeit, Geburtsort und -datum, Adresse des Wohnsitzes, E-Mail-Adresse und Telefonnummer, Nationalregisternummer, Nummer des Identitätsdokuments, Ausstellungsland bei ausländischen Dokumenten und Gültigkeitsdatum des Dokuments, Referenz des Zahlungsvorgangs, Verbindung der Guthabenkarte mit dem Produkt, für das der Endnutzer bereits identifiziert ist, und das Foto des Endnutzers, aber nur für andere Dokumente als den belgischen elektronischen Personalausweis. Wenn das Foto auf dem belgischen elektronischen Personalausweis dem Betreiber oder dem Identifizierungsdiensteanbieter übermittelt wurde, vernichten sie dieses Foto spätestens vor Aktivierung der Guthabenkarte.

Der königliche Erlass vom 27. November 2016 legt auch die gültigen Identifizierungsmethoden fest, nämlich die Identifizierung auf der Grundlage von Identifizierungsdokumenten in Anwesenheit des Endnutzers (Artikel 14), die Online-Identifizierung und die elektronische Signatur mit dem elektronischen Personalausweis beim betreffenden Unternehmen (Artikel 15), die Identifizierung über den Identifizierungsdiensteanbieter (Artikel 16), die Identifizierung auf der Grundlage des Online-Zahlungsvorgangs (Artikel 17), die Produkterweiterung oder -migration (Artikel 18) und die Überprüfung über elektronische Kommunikationsmittel (Artikel 19).

B.2.6. Während der Vorarbeiten wurde die Abschaffung der Anonymität bei Guthabenkarten wie folgt begründet:

« 1) En 2005, le législateur a introduit dans l'article 127, § 3, une dérogation pour les cartes prépayées par rapport à l'interdiction pour un opérateur d'offrir des services qui rendent difficile ou impossible l'identification de l'appelant. Il avait également prévu dans l'article 127, § 1er, une délégation au Roi pour que ce dernier fixe les modalités de l'identification des utilisateurs de cartes prépayées. L'intention du législateur était de mettre fin à l'anonymat pour les cartes prépayées.

2) Le législateur, en ne mettant pas directement fin à l'anonymat pour les cartes prépayées, avait pour but de favoriser la pénétration de la téléphonie mobile. Ce but est entièrement réalisé à l'heure actuelle.

3) La suppression de l'anonymat pour les cartes prépayées est une revendication déjà ancienne des autorités judiciaires (1999), des services de renseignement et de sécurité et des services d'urgence offrant de l'aide sur place. Pour ce qui concerne ces derniers, lors d'un appel

d'urgence, ils sont en droit d'obtenir de manière automatique et systématique les données d'identification de l'appelant telles que définies à l'article 2, 57°, de la LCE, dans l'intérêt de la sécurité du citoyen (voir l'article 107 de la LCE).

4) Les cartes prépayées sont très répandues dans les milieux criminels.

5) L'identification de l'utilisateur d'un service de communications électroniques est la première étape à franchir par la Justice ou les services de renseignement ou de sécurité, avant de procéder, le cas échéant, à d'autres mesures. Sans identification, ces autres mesures perdent une grande partie de leur utilité.

6) Actuellement, lorsque la Justice ou les services de renseignement ou de sécurité ne sont pas en mesure d'obtenir l'identification de l'utilisateur final dès lors que cet utilisateur a acheté une carte prépayée de manière anonyme, ils sont amenés à recourir à d'autres techniques pour tout de même identifier la personne recherchée. Ces autres techniques indirectes ont un coût plus important et sont plus intrusives dans la vie privée qu'une simple identification lors de l'achat d'une carte prépayée. Rendre plus efficace l'identification de la personne qui a souscrit à un service en supprimant l'anonymat pour les cartes prépayées a donc pour effet de diminuer les coûts pour la Justice et les services de renseignement et de sécurité (et le nombre de requêtes adressées aux opérateurs) et d'éviter une atteinte inutile à la vie privée de la personne en question et des personnes qui ont des liens avec cette dernière.

7) Comme le relève le Conseil d'État dans son avis n° 58.750/4 du 18 janvier 2016, il convient de relever d'une part, que seuls les acheteurs de cartes prépayées bénéficiaient, à ce jour, de l'anonymat, contrairement aux titulaires d'abonnement, et d'autre part que, dès l'adoption de la LCE, ce régime d'anonymat a été conçu comme destiné à recevoir un caractère temporaire. Dans ce contexte, la disposition à l'examen a donc pour conséquence, en droit et en fait, de rétablir un traitement non différencié entre les utilisateurs des services de communications électroniques concernés, et ainsi, de mettre fin à un traitement différencié temporaire plus favorable aux utilisateurs de cartes prépayées.

Les nouveaux alinéas 2 à 8 de l'article 127, § 1er, sont applicables à l'ensemble des services de communications électroniques. Par contre, le nouvel alinéa 2 introduit dans le paragraphe 3 de l'article 127 est spécifique aux services mobiles fournis sur la base d'une carte prépayée » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1964/001, SS. 4-6).

B.2.7. Dem Vorstehenden lässt sich entnehmen, dass die Identifizierbarkeit aller Endnutzer elektronischer Kommunikationsnetzwerke bereits von Anfang an der Ausgangspunkt von Artikel 127 des Gesetzes vom 13. Juni 2005 war und dass die Anonymität der Endnutzer von Guthabenkarten immer als zeitlich befristete Ausnahme aufgefasst wurde. Außerdem war es nicht so sehr der Gesetzgeber als vielmehr der König, der die Anonymität durch den königlichen Erlass vom 27. November 2016 abgeschafft hat.

B.3.1. Der durch Artikel 33 des angefochtenen Gesetzes abgeänderte Artikel 16/2 des Gesetzes vom 30. November 1998 bestimmt:

« Art. 16/2. § 1. Die Nachrichten- und Sicherheitsdienste können im Interesse der Erfüllung ihrer Aufträge die Mitwirkung eines Betreibers eines elektronischen Kommunikationsnetzes oder eines Anbieters eines elektronischen Kommunikationsdienstes anfordern, um Folgendes vorzunehmen:

1. die Identifizierung des Teilnehmers oder des gewöhnlichen Nutzers eines elektronischen Kommunikationsdienstes oder des benutzten elektronischen Kommunikationsmittels,

2. die Identifizierung der elektronischen Kommunikationsdienste und -mittel, die eine bestimmte Person über einen Festvertrag bezieht oder die gewöhnlich von einer bestimmten Person benutzt werden.

Die Anforderung erfolgt schriftlich durch den Dienstleiter oder seinen Beauftragten. Bei äußerster Dringlichkeit kann der Dienstleiter beziehungsweise sein Beauftragter diese Daten mündlich anfordern. Diese mündliche Anforderung wird binnen vierundzwanzig Stunden durch eine schriftliche Anforderung bestätigt.

Jeder Betreiber eines elektronischen Kommunikationsnetzes und jeder Anbieter eines elektronischen Kommunikationsdienstes, dessen Mitwirkung angefordert wird, verschafft dem Dienstleiter beziehungsweise seinem Beauftragten die angeforderten Daten innerhalb einer Frist und gemäß den Modalitäten, die durch Königlichen Erlass auf Vorschlag des Ministers der Justiz, des Ministers der Landesverteidigung und des für elektronische Kommunikation zuständigen Ministers festzulegen sind.

Der Dienstleiter beziehungsweise sein Beauftragter kann, unter Einhaltung der Verhältnismäßigkeits und Subsidiaritätsprinzipien und unter der Bedingung, dass die Abfrage aufgezeichnet wird, die erwähnten Daten zudem durch einen Zugriff auf die Dateien der Kunden des Betreibers beziehungsweise des Anbieters des Dienstes erhalten. Der König legt auf Vorschlag des Ministers der Justiz, des Ministers der Landesverteidigung und des für elektronische Kommunikation zuständigen Ministers die technischen Bedingungen fest, unter denen dieser Zugriff möglich ist.

§ 2. Die Nachrichten- und Sicherheitsdienste können im Interesse der Erfüllung ihrer Aufträge die Mitwirkung einer Bank oder eines Finanzinstituts anfordern, um die Identifizierung des Endnutzers einer in Artikel 127 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation erwähnten Guthabenkarte auf der Grundlage der Bezugsnummer eines elektronischen Bankgeschäfts vorzunehmen, das sich auf diese Guthabenkarte bezieht und vorher in Anwendung von § 1 von einem Betreiber oder einem Anbieter mitgeteilt worden ist.

Die Anforderung erfolgt schriftlich durch den Dienstleiter oder seinen Beauftragten. Bei äußerster Dringlichkeit kann der Dienstleiter beziehungsweise sein Beauftragter diese Daten mündlich anfordern. Diese mündliche Anforderung wird binnen vierundzwanzig Stunden durch eine schriftliche Anforderung bestätigt.

Jede Bank und jedes Finanzinstitut, dessen Mitwirkung angefordert wird, verschafft dem Dienstleiter beziehungsweise seinem Beauftragten unverzüglich die angeforderten Daten.

Die Identifizierungsdaten, die die Nachrichten- und Sicherheitsdienste im Rahmen der im vorliegenden Paragraphen erwähnten Vorgehensweise erhalten, sind auf die in § 1 erwähnten Identifizierungsdaten begrenzt.

§ 3. Wer sich weigert, die auf diese Weise angeforderten Daten mitzuteilen oder den angeforderten Zugriff zu verschaffen, wird mit einer Geldbuße von 26 bis zu 10.000 EUR belegt.

§ 4. Die Nachrichten- und Sicherheitsdienste führen ein Register aller angeforderten Identifizierungen und aller durch direkten Zugriff erhaltenen Identifizierungen. Der Ständige Ausschuss N erhält von dem betreffenden Nachrichten- und Sicherheitsdienst monatlich eine Liste der angeforderten Identifizierungen und aller Zugriffe ».

B.3.2. Die Identifizierung aufgrund des Online-Bankgeschäfts ist eine der gültigen Identifizierungsmethoden im Sinne des königlichen Erlasses vom 27. November 2016. Artikel 17 dieses königlichen Erlasses bestimmt/sieht vor:

« § 1. Betreffende Unternehmen können den Endnutzer auf der Grundlage eines elektronischen Online-Zahlungsvorgangs identifizieren, der spezifisch für den Kauf oder das Aufladen der Guthabenkarte ausgeführt wird.

Diese Methode unterliegt folgenden Bedingungen:

1. Der Zahlungsvorgang muss von einem in Artikel I.9 Nr. 2 Buchstabe *a), b), c)* und *d)* des Wirtschaftsgesetzbuches erwähnten Zahlungsdienstleister bearbeitet werden

2. Der Zahlungsdienstleister unterliegt dem Gesetz vom 11. Januar 1993 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung

3. Binnen achtzehn Monaten nach dem mit der Guthabenkarte verbundenen Zahlungsvorgang muss eine neue Identifizierung erfolgen

4. Der Endnutzer gibt in einem Online-Formular des betreffenden Unternehmens mindestens seinen Namen, seinen Vornamen, seinen Geburtsort und sein Geburtsdatum ein.

§ 2. Das betreffende Unternehmen speichert die Referenz des Zahlungsvorgangs und die Daten des Online-Formulars auf Vorrat ».

B.3.3. Während der Vorarbeiten wurde diese obligatorische Mitwirkung der Banken oder Finanzinstitute wie folgt begründet:

« L’arrêté royal relatif à l’identification de l’utilisateur final des services de communications électroniques publics mobiles fournis sur la base d’une carte prépayée

déterminera la manière dont un opérateur peut identifier ses utilisateurs finals. Cette identification peut entre autres se faire via une vérification sur la base d'une transaction bancaire en ligne.

Cette dernière méthode d'identification constitue la base de la présente proposition. L'identification via transaction bancaire implique que l'utilisateur final d'une carte prépayée (prepaid) puisse s'identifier sur la base d'une transaction bancaire électronique liée à la carte prépayée. Cette méthode est soumise à plusieurs conditions : (1) la transaction est liée à un compte bancaire dont l'identité du titulaire a préalablement été vérifiée. Cette méthode ne peut pas être appliquée en cas de carte bancaire non traçable, (2) la banque est établie en Belgique. L'opérateur concerné enregistre la référence de la transaction bancaire.

L'identification de l'utilisateur final d'une carte prépayée se fait via l'exercice de deux réquisitions :

1° une réquisition d'un opérateur d'un réseau de communications électroniques, pour l'obtention d'une donnée d'identification (en application de l'actuel article 16/2), à laquelle l'opérateur répond en donnant la référence d'une transaction bancaire, et

2° une réquisition d'une banque ou institution financière pour l'obtention de l'identité de la personne qui se cache derrière cette transaction bancaire (en application du nouveau § 2 de l'article 16/2).

Conformément à la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, la Sûreté de l'État et le Service général du renseignement et de la sécurité des Forces armées sont habilités à requérir un opérateur d'un réseau de communications électroniques ou un fournisseur d'un service de communications électroniques d'identifier l'abonné ou l'utilisateur habituel d'un service ou moyen de communication électronique.

Cette compétence (classée à l'origine dans la catégorie des ' méthodes spécifiques ') a été requalifiée, par la loi du 5 février 2016 modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice (la loi dite pot-pourri II), comme une méthode de renseignement ordinaire. Contrairement aux autres méthodes ordinaires, une série de conditions matérielles et formelles supplémentaires ont toutefois été fixées (compétence uniquement dans le chef du chef de service ou de son délégué et non dans le chef de tout agent de renseignement, enregistrement obligatoire) ainsi qu'un mécanisme de surveillance extérieur supplémentaire (notification mensuelle obligatoire du Comité permanent R qui à son tour en rend compte au Parlement et aux ministres compétents).

La sollicitation auprès d'une banque ou d'une institution financière d'informations sur les transactions bancaires par un service de renseignement et de sécurité (article 18/15 de la loi du 30 novembre 1998) n'est par contre possible que via la procédure définie dans la loi du 30 novembre 1998 d'application pour la catégorie des ' méthodes exceptionnelles '. Cette procédure nécessite un avis conforme préalable de la Commission BIM (la commission chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité) et l'autorisation du chef de service. Les méthodes exceptionnelles sont également soumises à des conditions d'application strictes.

Les différentes procédures auxquelles sont soumises les deux réquisitions font en sorte que la méthode d'identification via transaction bancaire (au fond une identification de l'utilisateur

d'un service de communications électroniques) devienne dans les faits une méthode exceptionnelle. C'est contraire à l'objectif poursuivi dans la loi Pot-pourri II.

En outre, il convient de garder à l'esprit que pour l'identification de l'utilisateur final d'une carte prépayée, l'information qui est demandée à la banque sert uniquement à retrouver l'identité de celui qui a effectué une transaction bancaire, et par conséquent, ne vise pas à avoir un aperçu de la situation financière de cette personne. Pour obtenir des informations concernant les comptes bancaires, le règlement actuel (méthode exceptionnelle) reste donc d'application. La méthode ordinaire permet de demander en d'autres termes uniquement le nom, le prénom, le sexe, la nationalité, le lieu et la date de naissance, l'adresse et le numéro de registre national de la personne qui est associée au numéro de compte en banque, et ce uniquement dans le cadre de l'identification de l'utilisateur d'une carte SIM prépayée.

Enfin, l'on peut souligner le fait que, dans la présente proposition, l'identification de l'utilisateur final d'une carte prépayée devient il est vrai une méthode ordinaire, mais qu'il y a tout de même des garanties supplémentaires par rapport à d'autres méthodes ordinaires. Ainsi, l'information ne peut pas être sollicitée par n'importe qui, mais seuls le chef de service ou son délégué y sont habilités. De plus, les services de renseignement et de sécurité tiennent un registre de toutes les identifications requises et doivent transmettre chaque mois une liste de ces réquisitions au Comité R » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1964/001, SS. 14-16).

In Bezug auf den ersten Klagegrund

B.4. Im ersten Klagegrund führen die klagenden Parteien an, dass Artikel 2 des angefochtenen Gesetzes gegen die Artikel 10, 11 und 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8 und 52 der Charta der Grundrechte der Europäischen Union (nachstehend: die Charta) und mit den Artikeln 2 Buchstabe a und 6 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 » verstoße, weil diese Bestimmung dem König eine zu weitreichende und nicht ausreichend genau bestimmte Ermächtigung erteile, um den Inhalt der angefochtenen Identifizierungsverpflichtung festzulegen.

B.5.1. Der Grundsatz der Gleichheit und Nichtdiskriminierung schließt nicht aus, dass ein Behandlungsunterschied zwischen Kategorien von Personen eingeführt wird, soweit dieser Unterschied auf einem objektiven Kriterium beruht und in angemessener Weise gerechtfertigt ist.

Das Vorliegen einer solchen Rechtfertigung ist im Hinblick auf Zweck und Folgen der beanstandeten Maßnahme sowie auf die Art der einschlägigen Grundsätze zu beurteilen; es wird gegen den Grundsatz der Gleichheit und Nichtdiskriminierung verstoßen, wenn feststeht, dass die eingesetzten Mittel in keinem angemessenen Verhältnis zum verfolgten Zweck stehen.

B.5.2. Artikel 22 der Verfassung bestimmt:

« Jeder hat ein Recht auf Achtung vor seinem Privat- und Familienleben, außer in den Fällen und unter den Bedingungen, die durch Gesetz festgelegt sind.

Das Gesetz, das Dekret oder die in Artikel 134 erwähnte Regel gewährleistet den Schutz dieses Rechtes ».

Artikel 8 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer ».

Artikel 7 der Charta bestimmt:

« Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation ».

Artikel 8 der Charta bestimmt:

« (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht ».

Artikel 52 Absatz 1 der Charta bestimmt:

« Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen ».

Artikel 52 Absatz 3 der Charta bestimmt:

« So weit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt ».

B.5.3. Der Verfassungsgeber hat eine möglichst weitgehende Übereinstimmung zwischen Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention angestrebt (*Parl. Dok.*, Kammer, 1992-1993, Nr. 997/5, S. 2).

Die Tragweite dieses Artikels 8 entspricht derjenigen der vorerwähnten Verfassungsbestimmung, sodass die durch die beiden Bestimmungen gebotenen Garantien ein untrennbares Ganzes bilden.

Wenn die Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte garantierten Rechten entsprechen, « haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird ». Diese Bestimmung bringt die Bedeutung und Tragweite der in der Charta garantierten Rechte mit den entsprechenden durch die Europäische Menschenrechtskonvention garantierten Rechten in Einklang.

In den Erläuterungen zur Charta (2007/C-303/02), die im *Amtsblatt* vom 14. Dezember 2007 veröffentlicht wurden, ist angegeben, dass unter den Artikeln, « die dieselbe Bedeutung und Tragweite wie die entsprechenden Artikel der Europäischen Menschenrechtskonvention haben », Artikel 7 der Charta Artikel 8 der Europäischen Menschenrechtskonvention entspricht.

Der Gerichtshof der Europäischen Union weist diesbezüglich darauf hin, dass « Art. 7 der Charta, der das Recht auf Achtung des Privat- und Familienlebens betrifft, Rechte enthält, die den in Art. 8 Abs. 1 [der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (nachstehend: EMRK)] gewährleisteten Rechten entsprechen, und dass somit Art. 7 der Charta gemäß Art. 52 Abs. 3 der Charta die gleiche Bedeutung und Tragweite beizumessen ist wie Art. 8 Abs. 1 EMRK in seiner Auslegung durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte » (EuGH, 17. Dezember 2015, C-419/14, *WebMindLicenses Kft.*, Randnrn. 70; 14. Februar 2019, C-345/17, *Buivids*, Randnr. 65).

In Bezug auf Artikel 8 der Charta ist der Gerichtshof der Auffassung, dass, « wie aus Art. 52 Abs. 3 Satz 2 der Charta hervorgeht, Art. 52 Abs. 3 Satz 1 der Charta dem nicht [entgegensteht], dass das Recht der Union einen weiter gehenden Schutz gewährt als die EMRK », und dass « Art. 8 der Charta ein anderes als das in ihrem Art. 7 verankerte Grundrecht [betrifft], für das es in der EMRK keine Entsprechung gibt » (EuGH, Große Kammer, 21. Dezember 2016, C-203/15 und C-698/15, *Tele2 Sverige*, Randnr. 129).

Aus dem Vorstehenden ergibt sich, dass innerhalb des Geltungsbereichs des Rechts der Europäischen Union Artikel 22 der Verfassung, Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 7 der Charta analoge Grundrechte gewährleisten, während Artikel 8 der Charta einen spezifischen Rechtsschutz für personenbezogene Daten bietet.

B.5.4. Gemäß Artikel 94 Absatz 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 « zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) » (nachstehend: Datenschutz-Grundverordnung) » wurde die Richtlinie 95/46/EG mit Wirkung vom 25. Mai 2018 aufgehoben.

Artikel 5 der Datenschutz-Grundverordnung, in dem *mutatis mutandis* der Wortlaut von Artikel 6 der Richtlinie 95/46/EG übernommen wurde, bestimmt:

« (1) Personenbezogene Daten müssen

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

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

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

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

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

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

2. Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (‘ Rechenschaftspflicht ’) ».

B.6. Indem Artikel 22 der Verfassung dem zuständigen Gesetzgeber die Befugnis vorbehält, festzulegen, in welchen Fällen und unter welchen Bedingungen das Recht auf Achtung des Privatlebens beeinträchtigt werden kann, gewährleistet er für jeden Bürger, dass keinerlei Einmischung in dieses Recht erfolgen kann, wenn dies nicht aufgrund von Regeln geschieht, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

Eine Ermächtigung der ausführenden Gewalt steht jedoch nicht im Widerspruch zum Legalitätsprinzip, sofern diese Ermächtigung ausreichend präzise beschrieben wird und sich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Gesetzgeber festgelegt wurden.

B.7.1. Nach Ansicht des Ministerrats ist der Klagegrund unzulässig, weil die angefochtene Bestimmung nur eine neue Ermächtigung zugunsten des Königs beinhalte, konkret die Ermächtigung, die in den neuen Artikel 127 § 3 Absatz 2 des Gesetzes vom 13. Juni 2005 eingefügt worden sei und die von den klagenden Parteien nicht angefochten werde. Die übrigen Ermächtigungen zugunsten des Königs seien bereits vor Inkrafttreten der angefochtenen Bestimmung Bestandteil von Artikel 127 dieses Gesetzes gewesen.

B.7.2. Eine Klage, die gegen einen Behandlungsunterschied gerichtet ist, der sich nicht aus dem angefochtenen Gesetz ergibt, sondern bereits in einem früheren Gesetz enthalten ist, ist unzulässig.

Wenn der Gesetzgeber in neuen Rechtsvorschriften jedoch eine alte Bestimmung übernimmt und sich auf diese Weise deren Inhalt zu eigen macht, kann gegen die übernommene Bestimmung eine Klage innerhalb von sechs Monaten nach deren Veröffentlichung eingereicht werden.

B.7.3. Die angefochtene Bestimmung hat Artikel 127 des Gesetzes vom 13. Juni 2005 an verschiedenen Stellen abgeändert, wenn auch der Gesetzgeber dabei, wie in B.2.7 ausgeführt wurde, dem ursprünglichen Ausgangspunkt der Identifizierbarkeit aller Endnutzer elektronischer Kommunikationsnetzwerke treu blieb. Dementsprechend hat er sich bei der Annahme der angefochtenen Bestimmung den Wortlaut von Artikel 127 des Gesetzes vom 13. Juni 2005 zu eigen gemacht.

Die Einrede wird abgewiesen.

B.8.1. Der Ausschuss für den Schutz des Privatlebens (jetzt die Datenschutzbehörde) hat in einer Stellungnahme zum Vorentwurf, der zum angefochtenen Gesetz geführt hat, einige Bemerkungen in Bezug auf die Einhaltung des Gesetzmäßigkeitsgrundsatzes bei Einschränkung des Rechts auf Achtung des Privatlebens formuliert:

« 10. L'avant-projet de loi règle spécifiquement cette question, ce qui permet de répondre à la condition de forme susmentionnée d'une base légale. La Commission constate cependant que le législateur a omis d'intégrer plusieurs éléments essentiels dans le texte légal. L'avant-projet de loi et l'Exposé des motifs renvoient tous les deux aux mesures d'exécution à prendre concernant les spécifications du traitement de données envisagé, qui seront définies par arrêté royal, à savoir la désignation du responsable du traitement, l'indication de qui a accès aux données, la définition du délai de conservation, … En l'absence de textes concrets, la Commission n'est actuellement pas en mesure d'émettre un avis sur les mesures d'exécution envisagées. La Commission souligne qu'une fois disponibles, les futurs arrêtés d'exécution (portant exécution de l'article 127 de la loi télécom) devront lui être préalablement soumis pour avis afin de pouvoir les confronter aux exigences de la loi vie privée, notamment en matière de proportionnalité. Il est recommandé d'intégrer cette demande d'avis préalable concernant les arrêtés d'exécution dans le texte législatif proprement dit.

[…]

14. Comme mentionné ci-avant […], la Commission recommande de préciser dans le texte législatif que l'identification des cartes prépayées achetées avant le 1er mai 2016 s'effectuera également au moyen des données d'identification devant être conservées en vertu de l'article 126. Il ne serait pas logique de prévoir d'autres catégories de données pour les utilisateurs existants. La nature des données doit être déterminée par la loi. L'arrêté d'exécution porte uniquement sur les mesures d'exécution et la date de mise en œuvre.

15. L'Exposé des motifs de l'avant-projet de loi explique en outre l'intention de compléter les données d'identification devant être conservées en vertu de l'article 126 avec le numéro de Registre national. Il est essentiel de reprendre cette explication telle quelle dans le texte législatif proprement dit.

[…]

PAR CES MOTIFS,

la Commission,

émet un avis favorable concernant l'avant-projet de loi modifiant la loi du 13 juin 2005 relative aux communications électroniques à la condition stricte qu'il soit tenu compte de ses remarques, et plus particulièrement celles visant :

- à lui soumettre pour avis les arrêtés d'exécution planifiés en vue notamment du contrôle de la proportionnalité (points 10 et 20);

- à mentionner explicitement dans la loi relative aux communications électroniques l'utilisation du numéro de Registre national, exclusivement en ce qui concerne les cartes prépayées (point 17);

- à préciser l'avant-projet de loi la nature des données, à savoir les données d'identification devant être conservées en vertu de l'article 126, complétées par le numéro de Registre national, et ce aussi bien pour les cartes achetées le 1er mai 2016 et après cette date, que pour les cartes

achetées avant cette date (points 14-15) » (ASP, Stellungnahme Nr. 54/2015, 15. Dezember 2015, *Parl. Dok.*, Kammer, 2015-2016, DOC 54-1964/001, SS. 38-42).

Auch die Gesetzgebungsabteilung des Staatsrats hat in einem Gutachten zu diesem Vorentwurf einige Bemerkungen über die Einhaltung des Gesetzmäßigkeitsgrundsatzes bei Einschränkung des Rechts auf Achtung des Privatlebens formuliert:

« 1.2.4. Les habilitations consenties au Roi par l'article 127, § 1er, alinéas 6 et 7 en projet sont excessivement larges : c'est au législateur qu'il appartient de déterminer les cas dans lesquels l'opérateur pourra ou devra faire une copie du document permettant d'établir l'identité de l'utilisateur final, de même que c'est à lui qu'il appartient de déterminer quel est ce document.

Par ailleurs, il convient que le législateur fixe les critères à mettre en œuvre par le Roi pour établir des méthodes d'identification différenciées, assorties de dates d'entrée en vigueur différenciées, selon que les cartes prépayées sont activées avant ou après une date fixée par le Roi. À cet égard, les explications figurant dans le commentaire de l'article gagneraient à être, pour l'essentiel, intégrées dans le dispositif en projet lui-même, sous la forme de critères à mettre en œuvre par le Roi, et pour le surplus, à être étoffées, dans le commentaire de l'article.

1.2.5. Si l'auteur de l'avant-projet a l'intention d'imposer la conservation non seulement des données d'identification – par définition, pendant le délai prévu à l'article 126 de la loi du 13 juin 2005 – mais également des documents ayant permis de recueillir ces données, c'est au législateur lui-même qu'il appartient d'imposer cette obligation et d'en déterminer le délai - lequel ne saurait évidemment être supérieur à celui prévu par l'article 126 » (Staatsrat, Gesetzgebungsabteilung, Gutachten Nr. 59.423/4, 15. Juni 2016, *Parl. Dok.*, Kammer, 2015-2016, DOC 54-1964/001, SS. 47-48).

B.8.2. Der Gesetzgeber hat diese Gutachten nur teilweise befolgt. Er hat sich insbesondere in Widerspruch zu diesen Gutachten dafür entschieden, in die angefochtene Bestimmung nicht aufzunehmen, welche Identifizierungsdaten gesammelt und verarbeitet werden dürfen und welche Identifizierungsdokumente berücksichtigt werden können. Diese Entscheidung wurde im Rahmen der Vorarbeiten wie folgt begründet:

« Premièrement, à l'exception de l'utilisation du numéro de registre national, c'est l'arrêté royal d'exécution de l'article 127, § 1er, alinéa 1er, de la loi (le projet d'arrêté royal ' cartes prépayées ') et non cet article qui définit les données d'identification à collecter.

En effet, les données d'identification précises à collecter, à l'exception du numéro de registre national, ne sont pas les éléments essentiels de la matière. D'ailleurs, la Commission de la protection de la vie privée, dans son premier avis sur le projet de loi (avis n° 54/2015 du 16 décembre 2015), ne demande pas que la liste des données à collecter soit reprise dans la loi mais uniquement d'indiquer ' la nature des données, à savoir les données d'identification devant être conservées en vertu de l'article 126 '. Pour répondre à la demande de la Commission

vie privée, le projet de loi prévoit que les données d'identification collectées sont conservées conformément à l'article 126, § 3, alinéa 1er, de la loi.

De plus, pour la conservation des données, c'est l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques et non l'article 126 qui fixe les données à conserver. Par analogie, c'est le projet d'arrêté royal ' cartes prépayées ' qui comprend les données d'identification à collecter et non l'article 127 de la loi, qui est la base légale de cet arrêté royal. Tant l'article 127 que l'article 126 constituent des restrictions aux libertés fondamentales.

Finalement, il n'est pas adéquat que la liste exacte des données d'identification à collecter soit reprise dans la loi, vu le caractère technique de ces données, le fait que ces données sont intimement liées aux méthodes d'identification développées dans l'arrêté royal ' cartes prépayées ' en projet (et ne peuvent être comprises qu'en lisant cet arrêté royal) et la nécessité éventuelle de les adapter à l'avenir en fonction des enseignements de la pratique ou des évolutions futures.

Deuxièmement, c'est le projet d'arrêté royal ' cartes prépayées ' et non l'article 127 de la loi qui déterminera la liste complète des documents d'identification qui sont acceptés.

En effet, il ne s'agit pas d'un élément essentiel de la législation (l'élément essentiel est par contre que l'identification doit se faire sur base d'un document d'identification valide).

Par ailleurs, reprendre cette liste dans la loi l'alourdirait (vu les nombreux documents d'identification qui devraient être admis) et aurait comme inconvénient de ne pas pouvoir facilement l'adapter en fonction des enseignements tirés de la pratique et des évolutions.

Troisièmement, le projet de loi ne développe pas de critères pour encadrer la délégation au Roi concernant la différenciation entre les nouvelles et les anciennes cartes prépayées comme demandé par le Conseil d'Etat. En effet, les méthodes d'identification pour les anciennes et les nouvelles cartes prépayées sont en réalité les mêmes : un utilisateur final d'une nouvelle carte prépayée et un utilisateur final d'une ancienne carte prépayée qui n'a pas encore été identifié doivent s'identifier selon les mêmes méthodes d'identification.

Par contre, le projet de loi fixe directement les règles applicables (voir le nouvel alinéa introduit au paragraphe 3 de l'article 127). La délégation au Roi ne portera plus que sur la définition de ce qu'est un utilisateur final d'une carte ancienne qui a déjà été identifié.

Par sa lettre du 1er juillet 2016 au Vice-Premier ministre et ministre des Télécommunications […], la Commission de la protection de la vie privée a indiqué ne pas avoir de commentaire sur ce projet » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1964/001, SS. 6-7).

B.8.3.1. Artikel 127 des Gesetzes vom 13. Juni 2005 regelt selbst das Prinzip der Identifizierbarkeit des Endnutzers, und zwar sowohl hinsichtlich alter als auch neuer Guthabenkarten. Er koppelt die Abschaffung der Anonymität bei Guthabenkarten an den Zeitpunkt, an dem der Ausführungserlass in Kraft tritt, und fügt dem hinzu, dass es ab diesem Zeitpunkt verboten ist, Dienste oder Ausrüstung bereitzustellen, die die Identifizierung

erschweren können. Er legt ebenso fest, dass vorbehaltlich des Beweises des Gegenteils der identifizierte Endnutzer als Nutzer des elektronischen Kommunikationsdienstes gilt.

Er erwähnt auch die Kategorien von Personen, denen in diesem Zusammenhang Verpflichtungen auferlegt werden, nämlich den Betreibern, den Anbietern, den Vertriebswegen, den Unternehmen, die einen Identifizierungsdienst anbieten, und den Endnutzern. Er legt schließlich auch das Ziel der Identifizierbarkeit fest, nämlich das gute Funktionieren der Notdienste, die strafrechtliche Untersuchung und das Funktionieren der Nachrichten- und Sicherheitsdienste.

B.8.3.2. Auf dem Gebiet der Identifizierbarkeit erteilt Artikel 127 des Gesetzes vom 13. Juni 2005 dem König verschiedene Ermächtigungen. Zunächst ermächtigt er Ihn auf allgemeine Weise, die technischen und administrativen Maßnahmen festzulegen, die in diesem Zusammenhang den betreffenden Parteien auferlegt werden müssen. Ebenso muss Er festlegen, wer die nicht identifizierten Endnutzer von Guthabenkarten sind, die vor Inkrafttreten des Ausführungserlasses gekauft wurden. Er muss auch die Höchstfrist festlegen, innerhalb deren sich die nicht identifizierten Endnutzer bei ihrem Betreiber identifizieren müssen, wenn auch Artikel 127 des Gesetzes von 13. Juni 2005 diese Ermächtigung eingrenzt, indem er festlegt, dass diese Frist einen Zeitraum von sechs Monaten nicht überschreiten darf. Schließlich muss der König die Tarife für die Mitwirkung der Betreiber und der Anbieter an der Identifizierung eines Endnutzers festlegen.

Diese Ermächtigungen beziehen sich auf die Umsetzung von Maßnahmen, deren wesentliche Elemente vorher vom Gesetzgeber festgelegt worden sind.

B.8.4.1. In Bezug auf die betreffenden Identifizierungsdaten und -dokumente bestimmt Artikel 127 des angefochtenen Gesetzes, dass es sich um Dokumente mit der Nationalregisternummer handeln muss sowie dass die Nationalregisternummer eine personenbezogene Information ist, die in diesem Zusammenhang zu sammeln und zu verarbeiten ist. Die übrigen Identifizierungsdaten sowie -dokumente, die berücksichtigt werden können, sind in Widerspruch zu den in B.8.1 erwähnten Gutachten nicht in dieser Gesetzesbestimmung genannt.

B.8.4.2. Außerdem hat der Gesetzgeber den König nicht ausdrücklich ermächtigt, diese Identifizierungsdaten und -dokumente näher zu bestimmen. Solche wesentlichen Elemente der Verarbeitung personenbezogener Daten können dabei nicht unter die unbestimmte Ermächtigung in Artikel 127 § 1 Absatz 1 des Gesetzes vom 13. Juni 2005 gefasst werden, die erforderlichen « technischen und administrativen Maßnahmen » im Hinblick auf die Identifizierbarkeit des Endnutzers festzulegen.

Der König musste diese Identifizierungsdaten und -dokumente folglich aufgrund der Befugnis festlegen, die ihm nach Artikel 108 der Verfassung zusteht, nämlich die zur Ausführung der Gesetze notwendigen Verordnungen und Erlasse zu erlassen.

Diese allgemeine Ausführungsbefugnis des Königs reicht vorliegend gleichwohl nicht aus. Die Ermächtigung hinsichtlich wesentlicher Elemente einer vom Verfassungsgeber dem formellen Gesetzgeber vorbehaltenen Angelegenheit ist nämlich nur dann möglich, wenn die Einhaltung des parlamentarischen Verfahrens es dem Gesetzgeber nicht ermöglichen würde, ein Ziel des Allgemeininteresses zu verwirklichen, und unter der Bedingung, dass er den Gegenstand dieser Ermächtigung ausdrücklich und unzweideutig festlegt und dass die vom König ergriffenen Maßnahmen von der gesetzgebenden Gewalt im Hinblick auf ihre Bestätigung innerhalb einer relativ kurzen, im Ermächtigungsgesetz vorgesehenen Frist geprüft werden.

B.8.4.3. In den Vorarbeiten begründet der Gesetzgeber diese Wiese des Vorgehens dadurch, dass er auf die technische Art der Identifizierungsdaten und -dokumente, die Notwendigkeit, die diesbezügliche Aufzählung im Lichte der geänderten Erkenntnisse anpassen zu können, und den Umstand verweist, dass auch im Rahmen der Vorratsdatenspeicherung diese Daten nicht im durch den Entscheid Nr. 57/2021 des Gerichtshofs vom 22. April 2021 für nichtig erklärten Artikel 126 des Gesetzes vom 13. Juni 2005 selbst aufgezählt wurden.

Abgesehen davon, dass diese Argumente das Fehlen einer ausdrücklichen und unzweideutigen Ermächtigung nicht erklären können, reicht die technische Art der Identifizierungsdaten und -dokumente sowie die Anpassungsfähigkeit einer solchen Aufzählung nicht aus, um schlussfolgern zu können, dass deren Verankerung in einer Gesetzesnorm es dem Gesetzgeber nicht ermöglichen würde, ein Ziel des Allgemeininteresses

zu verwirklichen. Auch eine Gesetzesnorm kann nämlich abgeändert werden. Der Ministerrat weist nicht nach, dass eine Abänderung dieser Identifizierungsdaten so dringend sein kann, dass der normale Ablauf des Gesetzgebungsverfahrens nicht eingehalten werden kann. Eine Aufzählung von Identifizierungsdaten und -dokumenten ist auch nicht derart komplex, dass sie nicht in eine Gesetzesnorm aufgenommen werden kann. Schließlich kann der Gesetzgeber einen Verstoß gegen die Verfassung nicht damit rechtfertigen, dass er auf eine andere Gesetzesbestimmung verweist, die womöglich mit der gleichen Verfassungswidrigkeit behaftet war.

B.8.4.4. Artikel 127 des Gesetzes vom 13. Juni 2005 grenzt die Ausführungsbefugnis des Königs bei der Bestimmung, welche Identifizierungsdaten gesammelt und verarbeitet werden und welche Identifizierungsdokumente berücksichtigt werden können, im Übrigen unzureichend ein. In Bezug auf die Identifizierungsdokumente erwähnt er nur, dass es sich um Dokumente handeln muss, die die Nationalregisternummer enthalten. In Bezug auf die anderen Identifizierungsdaten als die Nationalregisternummer enthält er keinerlei Präzisierung.

B.8.5. In Bezug auf das Sammeln und Verarbeiten der Identifizierungsdaten und -dokumente sieht Artikel 127 des Gesetzes vom 13. Juni 2005 vor, wer die Daten sammelt, nämlich der Vertriebsweg oder das Unternehmen, das einen Identifizierungsdienst anbietet. Er legt auch fest, dass der Vertriebsweg diese Daten und Dokumente nicht auf Vorrat speichern darf und sie spätestens zum Zeitpunkt der Aktivierung der Guthabenkarte vernichten muss.

In Bezug auf die Weise der Datenverarbeitung bestimmt Artikel 127 des Gesetzes vom 13. Juni 2005, wer der zuständige Datenverarbeiter ist, nämlich der Betreiber oder der Anbieter. Er bestimmt auch, dass der Vertriebsweg die gesammelten Daten dem Betreiber, dem Anbieter oder dem Unternehmen, das einen Identifizierungsdienst anbietet, durch unmittelbare Eingabe in ein Computersystem oder mittels einer Kopie des Identifizierungsdokuments übermittelt. Er sieht ebenso vor, dass der Betreiber und der Anbieter eine Kopie jedes anderen Identifizierungsdokuments als den belgischen elektronischen Personalausweis aufbewahren müssen und dass die verarbeiteten Identifizierungsdaten nach Artikel 126 § 3 des Gesetzes vom 13. Juni 2005 auf Vorrat zu speichern sind.

B.8.6. In Bezug auf die Sanktionen regelt Artikel 127 §§ 4 und 5 des Gesetzes vom 13. Juni 2005, dass Betreiber oder Anbieter, die die vom König auferlegten technischen und

administrativen Maßnahmen nicht umsetzen, den Dienst, auf den diese Maßnahmen anzuwenden sind, nicht mehr anbieten dürfen. Ebenso sieht er vor, dass die Endnutzer, die die ihnen auferlegten Verpflichtungen nicht erfüllen, ohne Entschädigung vom elektronischen Kommunikationsnetzwerk abzutrennen sind.

B.8.7.1. Die klagenden Parteien beanstanden ferner, dass die angefochtene Bestimmung keine separaten Kriterien für die Endnutzer alter Guthabenkarten und die Endnutzer neuer Guthabenkarten vorsehe.

Artikel 127 des Gesetzes vom 13. Juni 2005, abgeändert durch Artikel 2 des angefochtenen Gesetzes, unterwirft gleichwohl beide Kategorien von Endnutzern auf gleiche Weise dem Erfordernis der Identifizierbarkeit. Artikel 127 § 3 Absatz 2 dieses Gesetzes sieht in diesem Zusammenhang eine Höchstfrist vor, innerhalb deren die Endnutzer alter Guthabenkarten die vom König festgelegten administrativen und technischen Maßnahmen umsetzen müssen, während die neue Regelung ab dem Zeitpunkt ihres Inkrafttretens sofort auf neue Guthabenkarten angewandt wurde.

B.8.7.2. Sofern die klagenden Parteien hinsichtlich der angefochtenen Bestimmung beanstanden, dass sie nicht ausreichend klar bestimme, auf welche Kategorien von Endnutzern elektronischer Kommunikationsnetzwerke sie Anwendung finde, reicht es aus, festzustellen, dass in Übereinstimmung mit dem ursprünglichen Ziel von Artikel 127 des Gesetzes vom 13. Juni 2005 alle Endnutzer in ihren Anwendungsbereich fallen, unabhängig davon, ob sie über einen Festvertrag verfügen oder eine Guthabenkarte verwenden. Wie in B.2.6 ausgeführt wurde, ist die Angleichung der Endnutzer einer Guthabenkarte an die Inhaber eines Festvertrags im Übrigen eines der Ziele des angefochtenen Gesetzes.

B.8.7.3. Sofern die klagenden Parteien hinsichtlich der angefochtenen Bestimmung beanstanden, dass sie die Umstände der Datenverarbeitung nicht präzisiere, ist festzustellen, dass sie in diesem Zusammenhang auf Artikel 126 § 3 des Gesetzes vom 13. Juni 2005 verweist.

In seinem Entscheid Nr. 57/2021 vom 22. April 2021 hat der Gerichtshof unter anderem Artikel 4 des Gesetzes vom 29. Mai 2016 « über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation » für nichtig erklärt. Bereits in seinem

Entscheid Nr. 84/2015 vom 11. Juni 2015 hatte der Gerichtshof 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 » für nichtig erklärt. Infolge dieser Entscheide ist Artikel 126 des Gesetzes vom 13. Juni 2005 jetzt anwendbar in der Fassung, die zuletzt durch Artikel 33 des Gesetzes vom 4. Februar 2010 « über die Methoden zum Sammeln von Daten durch die Nachrichten- und Sicherheitsdienste » abgeändert wurde. Die erwähnten Nichtigerklärungen beruhten im Wesentlichen auf dem Verbot einer allgemeinen und unterschiedslosen Aufbewahrung von Daten. Unter Berücksichtigung der unionsrechtlichen Grundlage dieses Verbots kann nicht angenommen werden, dass Artikel 126 des Gesetzes vom 13. Juni 2005 in der Fassung anwendbar ist, die vor diesen Nichtigerklärungen galt, sofern sie sich auf eine allgemeine und unterschiedslose Aufbewahrung von Daten im Bereich der elektronischen Kommunikation bezieht. Dieselbe Bestimmung kann dahingegen angewandt werden, sofern sie sich auf die Identifizierungsdaten von Nutzern von Guthabenkarten im Sinne von Artikel 127 desselben Gesetzes bezieht. Artikel 126, abgeändert durch das Gesetz vom 4. Februar 2010, bestimmt:

« § 1. 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 Bedingungen fest, unter denen Betreiber im Hinblick auf Verfolgung und Ahndung strafrechtlicher Verstöße, auf die Ahndung böswilliger Anrufe bei Hilfsdiensten und auf die vom Ombudsdienst für Telekommunikation geführte Ermittlung der Identität von Personen, die elektronische Kommunikationsnetze beziehungsweise -dienste böswillig genutzt haben, sowie im Hinblick auf die Erfüllung der im Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten nachrichtendienstlichen Aufträge Verkehrs- und Identifizierungsdaten von Endnutzern aufzeichnen und aufbewahren.

§ 2. Aufzubewahrende Daten und Dauer dieser Aufbewahrung, die bei öffentlich zugänglichen Telefondiensten zwischen zwölf und sechsunddreißig Monaten liegen muss, werden vom König nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts durch einen im Ministerrat beratenen Erlass festgelegt.

Betreiber gewährleisten, dass die in § 1 erwähnten Daten von Belgien aus unbeschränkt zugänglich sind ».

Zur Ausführung dieser Bestimmung regelt der königliche Erlass vom 19. September 2013 « zur Ausführung von Artikel 126 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation » (nachstehend: königlicher Erlass vom 19. September 2013) jetzt die Verarbeitung und die Aufbewahrung personenbezogener Daten, auch in Bezug auf die

Identifizierungsdaten, die aufgrund von Artikel 127 des Gesetzes vom 13. Juni 2005 gesammelt werden.

In seinem Ergänzungsschriftsatz und in der Sitzung hat der Ministerrat im Übrigen darauf hingewiesen, dass eine neue Fassung von Artikel 126 des Gesetzes vom 13. Juni 2005 vorbereitet wird, um die Anforderungen aus dem Entscheid Nr. 57/2021 des Gerichtshofs zu erfüllen und die darin angewandte Rechtsprechung des Gerichtshofs der Europäischen Union umzusetzen.

B.8.7.4. Sofern die klagenden Parteien hinsichtlich der angefochtenen Bestimmung beanstanden, dass sie nicht regle, wer auf die gespeicherten Identifizierungsdaten zugreifen und auf der Grundlage welcher Bedingungen dies erfolgen könne, reicht es aus, festzustellen, dass dieser Zugriff nicht durch Artikel 127 des Gesetzes vom 13. Juni 2005 geregelt wird, sondern durch die Artikel 46*bis*, 88*bis* und 90*ter* bis 90*decies* des Strafprozessgesetzbuches hinsichtlich des Zugriffs im Rahmen einer strafrechtlichen Untersuchung, durch Artikel 16/2 § 1 des Gesetzes vom 30. November 1998 hinsichtlich des Zugriffs durch die Nachrichten- und Sicherheitsdienste und durch Artikel 107 § 2 des Gesetzes vom 13. Juni 2005 hinsichtlich des Zugriffs durch die Notdienste.

B.8.8. Außerdem konnte der Gesetzgeber, indem er eine solche Ermächtigung erteilte, den König nicht ermächtigen, Bestimmungen anzunehmen, die zu einem Verstoß gegen das Recht auf Achtung des Privatlebens führen würden. Es obliegt dem zuständigen Richter zu prüfen, ob der König auf gesetzmäßige Weise von der Ihm erteilten Ermächtigung Gebrauch gemacht hat.

B.9.1. Aus dem Vorstehenden ergibt sich, dass Artikel 127 des Gesetzes vom 13. Juni 2005, abgeändert durch Artikel 2 des angefochtenen Gesetzes, den durch Artikel 22 der Verfassung garantieren Gesetzmäßigkeitsgrundsatz verletzt, wenn auch nur in dem Umfang, in dem er nicht bestimmt, welche Identifizierungsdaten gesammelt und verarbeitet werden und welche Identifizierungsdokumente berücksichtigt werden können. In diesem Umfang ist Artikel 2 des angefochtenen Gesetzes für nichtig zu erklären.

Im Übrigen ist der erste Klagegrund unbegründet, da sich die angefochtenen Ermächtigungen zugunsten des Königs auf die Ausführung von Maßnahmen beziehen, deren wesentliche Elemente vorher vom Gesetzgeber bestimmt worden sind.

B.9.2. Im Gegensatz zum Vorbringen der klagenden Parteien hat der Europäische Gerichtshof für Menschenrechte in seinem Entscheid *Rotaru* nicht entschieden, dass die Verarbeitung personenbezogener Daten und der Zugriff auf die verarbeiteten Daten durch die gesetzgebende Gewalt zu regeln sind. Er hat nur betont, dass diese Verarbeitung und dieser Zugriff eine klare, zugängliche und vorhersehbare Grundlage im innerstaatlichen Recht haben müssen (EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, §§ 47-63).

Auch der Gerichtshof der Europäischen Union verlangt nur, dass « die gesetzliche Grundlage für den Eingriff in [das Recht auf Achtung des Privatlebens] den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, selbst festlegen muss » (EuGH, 6. Oktober 2020, C-623/17, *Privacy International*, Randnr. 65). Er verlangt nicht, dass alle Aspekte dieser Einschränkung durch formelles Gesetz geregelt werden.

Eine Prüfung der angefochtenen Bestimmung anhand von Artikel 8 der Europäischen Menschenrechtskonvention, der Artikel 7 und 8 der Charta oder von Artikel 5 der Datenschutz-Grundverordnung führt folglich zu keinem anderen Ergebnis, da sich aus diesen Bestimmungen keine strengeren Anforderungen in Bezug auf den formellen Gesetzmäßigkeitsgrundsatz ergeben als aus Artikel 22 der Verfassung.

B.9.3. Da sich der festgestellte Verstoß nur auf Artikel 22 der Verfassung und nicht auf die im Klagegrund angeführten Normen des Rechts der Europäischen Union bezieht, obliegt es dem Gerichtshof, nach Artikel 8 Absatz 3 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof die Folgen der für nichtig erklärten Bestimmungen zu bestimmen, die als aufrechterhalten anzusehen sind oder während der Frist, die er festlegt, vorläufig aufrechterhalten werden.

Der festgestellte Verstoß gegen Artikel 22 der Verfassung bezieht sich nicht auf die Art und den Inhalt der Identifizierungsdaten oder -dokumente, wie sie zurzeit im königlichen Erlass vom 27. November 2016 geregelt sind, und die nicht in die Prüfungsbefugnis des Gerichtshofs fallen. Er bezieht sich nur auf den Umstand, dass diese Daten und Dokumente in einer Gesetzesbestimmung hätten angeführt werden müssen.

Dem Gesetzgeber ist folglich die notwendige Zeit einzuräumen, um diese gesetzliche Grundlage zu schaffen, ohne dass in der Zwischenzeit die durch die angefochtene Bestimmung geregelte Identifizierung der Endnutzer von Guthabenkarten für nichtig erklärt werden muss. Diese Frist muss darüber hinaus ausreichend lang sein, um es dem Gesetzgeber zu ermöglichen, diese gesetzliche Grundlage auf die neue Regelung zur Vorratsdatenspeicherung abstimmen, die aufgrund des Entscheids Nr. 57/2021 des Gerichthofs vom 22. April 2021 vorbereitet wird.

Folglich sind die Folgen der angefochtenen Bestimmung in dem im Tenor angegebenen Maße aufrechtzuerhalten.

In Bezug auf den zweiten Klagegrund

B.10. Im zweiten Klagegrund führen die klagenden Parteien an, dass die Artikel 2 und 3 des angefochtenen Gesetzes gegen die Artikel 10, 11, 19, 22 und 25 der Verfassung in Verbindung mit den Artikeln 8 und 10 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11 und 52 der Charta, mit den Artikeln 56 und 57 des Vertrags über die Arbeitsweise der Europäischen Union, mit den Artikeln 2 Buchstabe b und 6 der Richtlinie 95/46/EG und mit den Artikeln 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) » verstoße. Dieser Klagegrund setzt sich aus drei Teilen zusammen.

B.11.1. Artikel 19 der Verfassung bestimmt:

« Die Freiheit der Kulte, diejenige ihrer öffentlichen Ausübung sowie die Freiheit, zu allem seine Ansichten kundzutun, werden gewährleistet, unbeschadet der Ahndung der bei der Ausübung dieser Freiheiten begangenen Delikte ».

Artikel 25 der Verfassung bestimmt:

« Die Presse ist frei; die Zensur darf nie eingeführt werden; von den Autoren, Verlegern oder Druckern darf keine Sicherheitsleistung verlangt werden.

Wenn der Autor bekannt ist und seinen Wohnsitz in Belgien hat, darf der Verleger, Drucker oder Verteiler nicht verfolgt werden ».

Artikel 10 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. Dieser Artikel hindert die Staaten nicht, für Radio-, Fernseh- oder Kinounternehmen eine Genehmigung vorzuschreiben.

(2) Die Ausübung dieser Freiheiten ist mit Pflichten und Verantwortung verbunden; sie kann daher Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung ».

Artikel 11 der Charta bestimmt:

« (1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben.

(2) Die Freiheit der Medien und ihre Pluralität werden geachtet ».

Insofern darin das Recht auf Freiheit der Meinungsäußerung anerkannt wird, haben Artikel 10 der Europäischen Menschenrechtskonvention und Artikel 11 Absatz 1 der Charta eine gleichartige Tragweite wie Artikel 19 der Verfassung, in dem die Freiheit anerkannt wird, zu allem seine Ansichten kundzutun.

Folglich bilden die durch diese Bestimmungen gebotenen Garantien insofern ein untrennbares Ganzes.

B.11.2. Artikel 56 des Vertrags über die Arbeitsweise der Europäischen Union bestimmt:

« Die Beschränkungen des freien Dienstleistungsverkehrs innerhalb der Union für Angehörige der Mitgliedstaaten, die in einem anderen Mitgliedstaat als demjenigen des Leistungsempfängers ansässig sind, sind nach Maßgabe der folgenden Bestimmungen verboten.

Das Europäische Parlament und der Rat können gemäß dem ordentlichen Gesetzgebungsverfahren beschließen, dass dieses Kapitel auch auf Erbringer von Dienstleistungen Anwendung findet, welche die Staatsangehörigkeit eines dritten Landes besitzen und innerhalb der Union ansässig sind ».

Artikel 57 des Vertrags über die Arbeitsweise der Europäischen Union bestimmt:

« Dienstleistungen im Sinne der Verträge sind Leistungen, die in der Regel gegen Entgelt erbracht werden, soweit sie nicht den Vorschriften über den freien Waren- und Kapitalverkehr und über die Freizügigkeit der Personen unterliegen.

Als Dienstleistungen gelten insbesondere:

a) gewerbliche Tätigkeiten,

b) kaufmännische Tätigkeiten,

c) handwerkliche Tätigkeiten,

d) freiberufliche Tätigkeiten.

Unbeschadet des Kapitels über die Niederlassungsfreiheit kann der Leistende zwecks Erbringung seiner Leistungen seine Tätigkeit vorübergehend in dem Mitgliedstaat ausüben, in dem die Leistung erbracht wird, und zwar unter den Voraussetzungen, welche dieser Mitgliedstaat für seine eigenen Angehörigen vorschreibt ».

B.11.3. Die Artikel 1, 2, 3, 5, 6, 9 und 15 der Richtlinie 2002/58/EG bestimmen:

« Artikel 1. Geltungsbereich und Zielsetzung

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

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

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des

Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.

Artikel 2. Begriffsbestimmungen

Sofern nicht anders angegeben, gelten die Begriffsbestimmungen der Richtlinie 95/46/EG und der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (‘ Rahmenrichtlinie ’) auch für diese Richtlinie.

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

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

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

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

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

f) ‘ Einwilligung ’ eines Nutzers oder Teilnehmers die Einwilligung der betroffenen Person im Sinne von Richtlinie 95/46/EG;

g) ‘ Dienst mit Zusatznutzen ’ jeden Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht;

h) ‘ elektronische Post ’ jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird;

i) ‘ Verletzung des Schutzes personenbezogener Daten ’ eine Verletzung der Sicherheit, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung und zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in der Gemeinschaft verarbeitet werden.

Artikel 3. Betroffene Dienste

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

[…]

Artikel 5. Vertraulichkeit der Kommunikation

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

(2) Absatz 1 betrifft nicht das rechtlich zulässige Aufzeichnen von Nachrichten und der damit verbundenen Verkehrsdaten, wenn dies im Rahmen einer rechtmäßigen Geschäftspraxis zum Nachweis einer kommerziellen Transaktion oder einer sonstigen geschäftlichen Nachricht geschieht.

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

Artikel 6. Verkehrsdaten

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

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

(3) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann die in Absatz1 genannten Daten zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu oder zur Vermarktung erforderlichen Zeitraums verarbeiten, sofern der Teilnehmer oder der Nutzer, auf den sich die Daten beziehen, zuvor seine Einwilligung gegeben hat. Der Nutzer oder der Teilnehmer hat die Möglichkeit, seine Einwilligung zur Verarbeitung der Verkehrsdaten jederzeit zu widerrufen.

(4) Der Diensteanbieter muss dem Teilnehmer oder Nutzer mitteilen, welche Arten von Verkehrsdaten für die in Absatz 2 genannten Zwecke verarbeitet werden und wie lange das geschieht; bei einer Verarbeitung für die in Absatz 3 genannten Zwecke muss diese Mitteilung erfolgen, bevor um Einwilligung ersucht wird.

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

(6) Die Absätze 1, 2, 3 und 5 gelten unbeschadet der Möglichkeit der zuständigen Gremien, in Einklang mit den geltenden Rechtsvorschriften für die Beilegung von Streitigkeiten, insbesondere Zusammenschaltungs- oder Abrechnungsstreitigkeiten, von Verkehrsdaten Kenntnis zu erhalten.

[…]

Artikel 9. Andere Standortdaten als Verkehrsdaten

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

(2) Haben die Nutzer oder Teilnehmer ihre Einwilligung zur Verarbeitung von anderen Standortdaten als Verkehrsdaten gegeben, dann müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und gebührenfrei zeitweise zu untersagen.

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie

auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Kommunikationsnetzes oder öffentlich zugänglichen Kommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

[…]

Artikel 15. Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG

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

(1a) Absatz 1 gilt nicht für Daten, für die in der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben ist.

(1b) Die Anbieter richten nach den gemäß Absatz 1 eingeführten nationalen Vorschriften interne Verfahren zur Beantwortung von Anfragen über den Zugang zu den personenbezogenen Daten der Nutzer ein. Sie stellen den zuständigen nationalen Behörden auf Anfrage Informationen über diese Verfahren, die Zahl der eingegangenen Anfragen, die vorgebrachten rechtlichen Begründungen und ihrer Antworten zur Verfügung.

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

(3) Die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Datenschutzgruppe nimmt auch die in Artikel 30 jener Richtlinie festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr ».

In Bezug auf den ersten Teil des zweiten Klagegrunds

B.12. Im ersten Teil des zweiten Klagegrundes führen die klagenden Parteien an, dass die allgemeine und unterschiedslose Identifizierungspflicht für alle Endnutzer elektronischer Kommunikationsdienste, die das angefochtene Gesetz ins Leben rufe, einen Eingriff in das Recht auf Achtung des Privatlebens darstelle, der über das hinausgehe, was im Lichte der verfolgten Ziele notwendig sei.

B.13.1. Das Recht auf Achtung des Privatlebens ist nicht absolut. Die angeführten Verfassungs- und internationalen Bestimmungen schließen einen staatlichen Eingriff in das Recht auf Achtung des Privatlebens nicht aus, schreiben aber vor, dass ein solcher Eingriff durch eine hinreichend genaue Gesetzesbestimmung erlaubt wird, dass dieser einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entspricht sowie im Verhältnis zum damit verfolgten gesetzlichen Ziel steht.

Der Gesetzgeber besitzt diesbezüglich einen Ermessensspielraum. Dieser Ermessensspielraum ist jedoch nicht unbegrenzt; damit eine gesetzliche Regelung mit dem Recht auf Achtung des Privatlebens vereinbar ist, ist es erforderlich, dass der Gesetzgeber ein faires Gleichgewicht zwischen allen betroffenen Rechten und Interessen gefunden hat. Bei der Beurteilung dieses Gleichgewichts berücksichtigt der Europäische Gerichtshof für Menschenrechte unter anderem die Bestimmungen des Übereinkommens des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und die Empfehlung Nr. R (87) 15 des Ministerkomitees an die Vertragsstaaten über die Nutzung personenbezogener Daten im Polizeibereich (EuGHMR, 25. Februar 1997, *Z gegen Finnland*, § 95; Große Kammer, 4. Dezember 2008, 2010, *S. und Marper gegen Vereinigtes Königreich*, § 103).

B.13.2. Bei der Beurteilung der Verhältnismäßigkeit von Maßnahmen in Bezug auf die Verarbeitung personenbezogener Daten sind u.a. deren automatischer Charakter, die verwendeten Techniken, der Genauigkeitsgrad, die Relevanz, der gegebenenfalls außergewöhnliche Charakter der zu verarbeitenden Daten, das etwaige Vorhandensein von Maßnahmen zur Begrenzung der Datenspeicherfrist, das etwaige Vorhandensein eines unabhängigen Überwachungssystems, mit dem geprüft werden kann, ob eine Datenspeicherung weiterhin erforderlich ist, das etwaige Vorhandensein von ausreichenden Kontrollrechten und

Rechtsbehelfen für die betroffenen Personen, das etwaige Vorhandensein von Garantien zur Vermeidung einer Stigmatisierung der Personen, deren Daten verarbeitet werden, der unterscheidende Charakter der Regelung und das etwaige Vorhandensein von Garantien zur Vermeidung einer falschen Nutzung und von Missbrauch der verarbeiteten personenbezogenen Daten durch öffentliche Behörden zu berücksichtigen (Entscheid Nr. 108/2016 vom 14. Juli 2016, B.12.2; Entscheid Nr. 29/2018 vom 15. März 2018, B.14.4; Entscheid Nr. 27/2020 vom 20. Februar 2020, B.8.3; EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, § 59; Entscheidung, 29. Juni 2006, *Weber und Saravia gegen Deutschland*, § 135; 28. April 2009, *K.H. u.a. gegen Slowakei*, §§ 60-69; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, §§ 101-103, 119, 122 und 124; 18. April 2013, *M.K. gegen Frankreich*, §§ 37 und 42-44; 18. September 2014, *Brunet gegen Frankreich*, §§ 35-37; 12. Januar 2016, *Szabó und Vissy gegen Ungarn*, § 68; 30. Januar 2020, *Breyer gegen Deutschland*, §§ 73-80; Große Kammer, 25. Mai 2021, *Centrum för rättvisa gegen Schweden*, §§ 262-278; Große Kammer, 25. Mai 2021, *Big Brother Watch gegen Vereinigtes Königreich*, §§ 348-364; EuGH, Große Kammer, 8. April 2014, C-293/12, *Digital Rights Ireland Ltd*, und C-594/12, *Kärntner Landesregierung u.a.*, Randnrn. 56-66); Große Kammer, 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, Randnrn. 105-133; Große Kammer, 6. Oktober 2020, C-623/17, *Privacy International*, Randnrn. 58-82; Große Kammer, 2. März 2021, C-746/18, *Prokuratuur*, Randnrn. 50-56).

B.13.3. Aus der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte geht hervor, dass personenbezogene Daten nicht länger als notwendig für die Verwirklichung des Ziels, zu dem sie gespeichert werden, in einer Form aufbewahrt werden dürfen, die eine Identifizierung zulässt oder die zulässt, eine Verbindung zwischen einer Person und strafbaren Handlungen herzustellen. Bei der Beurteilung der Verhältnismäßigkeit der Dauer der Aufbewahrung in Bezug auf den Zweck, zu dem die Daten gespeichert wurden, berücksichtigt der Europäische Gerichtshof für Menschenrechte den Umstand, ob eine unabhängige Kontrolle über die Rechtfertigung für die Bewahrung der Daten in den Datenbanken anhand deutlicher Kriterien besteht oder nicht, so wie die Schwere der Taten, den Umstand, ob die betreffende Person früher bereits Gegenstand einer Festnahme war, die Schwere der auf einer Person ruhenden Verdächtigungen sowie jeder andere besondere Umstand (EuGHMR, Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, § 103; 18. April 2013, *M.K. gegen Frankreich*, § 35; 17. Dezember 2009, *B.B. gegen Frankreich*, § 61; 18. September 2014, *Brunet gegen Frankreich*, §§ 35-40).

B.14.1. In Bezug auf das allgemeine und unterschiedslose Sammeln, Verarbeiten und Aufbewahren personenbezogener Daten der Nutzer elektronischer Kommunikationsnetzwerke unterscheiden sowohl der Europäische Gerichtshof für Menschenrechte als auch der Gerichtshof der Europäischen Union zwischen Verkehrs- und Standortdaten einerseits und Identifizierungsdaten andererseits.

B.14.2. Sie sehen das Sammeln, Verarbeiten und Aufbewahren von Verkehrs- und Standortdaten dieser Nutzer als eine sehr weitreichende Einschränkung des Rechts auf Achtung des Privatlebens an, da solche Daten sensible Informationen über eine Vielzahl von Aspekten des Privatlebens der betroffenen Personen enthalten können, wie deren sexuelle Orientierung, politische Meinungen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen sowie ihren Gesundheitszustand.

Aus solchen 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. Anhand dieser Informationen lässt sich ein Profil der betroffenen Personen erstellen, was ebenso sensibel ist wie der Inhalt der Kommunikationen selbst (EuGHMR, Große Kammer, 25. Mai 2021, *Centrum för rättvisa gegen Schweden*, §§ 238-245; Große Kammer, 25. Mai 2021, *Big Brother Watch gegen Vereinigtes Königreich*, §§ 324-331; EuGH, Große Kammer, 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, Randnr. 117; Große Kammer, 6. Oktober 2020, C-623/17, *Privacy International*, Randnr. 71).

Der Gerichtshof der Europäischen Union leitet daraus ab, dass das allgemeine und unterschiedslose Sammeln, Verarbeiten und Aufbewahren von Verkehrs- und Standortdaten grundsätzlich verboten ist. Dies ist nur aus Gründen der nationalen Sicherheit erlaubt und nur, sofern hinreichend konkrete Umstände die Annahme zulassen, dass sich der betreffende Mitgliedstaat einer als real, aktuell und vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht. Außerdem muss diese Aufbewahrung im Lichte dieser Bedrohung für die nationale Sicherheit in zeitlicher Hinsicht auf das absolut Notwendige beschränkt werden und muss sie mit strengen Garantien verbunden sein, die einen wirksamen

Schutz der personenbezogenen Daten vor Missbrauchsrisiken ermöglichen, unter anderem durch eine wirksame Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle (EuGH, Große Kammer, 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, Randnrn. 137-139). Das Sammeln, Verarbeiten und Aufbewahren von Verkehrs- und Standortdaten zum Zwecke der Bekämpfung schwerer Kriminalität darf hingegen keinen allgemeinen und unterschiedslosen Charakter haben, sondern muss auf der Grundlage eines geografischen oder personenbezogenen Kriteriums eingegrenzt werden (ebenda, Randnrn. 144-150).

Demgegenüber verbietet der Europäische Gerichtshof für Menschenrechte das allgemeine und unterschiedslose Sammeln, Verarbeiten und Aufbewahren von Verkehrs- und Standortdaten nicht, sondern unterwirft es einer strengen Prüfung. Er beurteilt die Rechtmäßigkeit und die Notwendigkeit solcher Maßnahmen in einer demokratischen Gesellschaft anhand des Grundes, aus dem die « Massenüberwachung » angeordnet wird, der Umstände beim Abfangen der Kommunikation von Privatpersonen, des Verfahrens, mit dem die Massenüberwachung erlaubt wird, des Verfahrens, mit dem das zu verwendende Material ausgewählt wird, der Schutzmaßnahmen, die ergriffen werden, wenn die verarbeiteten Daten an Dritte weitergegeben werden, der Frist, die für das Abfangen und das Aufbewahren personenbezogener Daten gilt, einschließlich der Umstände, unter denen die Daten vernichtet werden, des Verfahrens und der Modalitäten der vorherigen Kontrolle durch eine unabhängige Stelle hinsichtlich der Einhaltung der Garantien, einschließlich der von dieser Stelle gebotenen rechtlichen Wiedergutmachung, und des Verfahrens der unabhängigen nachträglichen Überprüfung hinsichtlich der Einhaltung aller einschlägigen Regeln (EuGHMR, Große Kammer, 25. Mai 2021, *Centrum för rättvisa gegen Schweden*, § 275; Große Kammer, 25. Mai 2021, *Big Brother Watch gegen Vereinigtes Königreich*, § 361).

B.14.3. Hingegen sehen der Europäische Gerichtshof für Menschenrechte und der Gerichtshof der Europäischen Union das allgemeine und unterschiedslose Sammeln, Verarbeiten und Aufbewahren bloßer Identifizierungsdaten von Nutzern elektronischer Kommunikationsnetzwerke als eine weniger einschneidende Einschränkung des Recht auf Achtung des Privatlebens an, da diese Daten es für sich genommen weder ermöglichen, das Datum, die Uhrzeit, die Dauer und die Adressaten der Kommunikation in Erfahrung zu bringen, noch die Orte, an denen sie stattfanden, oder wie häufig dies mit bestimmten Personen innerhalb eines gegebenen Zeitraums geschah. Diese Daten liefern daher keine Informationen über die

konkreten Kommunikationen dieser Personen und infolgedessen über ihr Privatleben. Anhand nur dieser Daten lässt sich weder ein Profil des Nutzers erstellen noch können seine Bewegungen verfolgt werden (EuGHMR, 30. Januar 2020, *Breyer gegen Deutschland*, §§ 92-95; EuGH, 2. Oktober 2018, C-207/16, *Ministerio Fiscal*, Randnr. 62; Große Kammer, 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, Randnr. 157).

Der Gerichtshof der Europäischen Union leitet daraus ab, dass das Recht auf Achtung des Privatlebens einem allgemeinen und unterschiedslosen Sammeln, Verarbeiten und Aufbewahren von Identifizierungsdaten von Nutzern elektronischer Kommunikationsnetzwerke zur Ermittlung, Feststellung und Verfolgung von Straftaten sowie zum Schutz der öffentlichen Sicherheit nicht entgegensteht. Dabei muss es sich nicht um schwere Straftaten, Bedrohungen oder Beeinträchtigungen der öffentlichen Sicherheit handeln (EuGH, Große Kammer, 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, Randnr. 159). Allerdings muss der Nachweis erbracht werden, dass « diese Rechtsvorschriften […] 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 » (ebenda, Randnr. 168).

Der Europäische Gerichtshof für Menschenrechte prüft das allgemeine und unterschiedslose Sammeln, Verarbeiten und Aufbewahren dieser Identifizierungsdaten auf weniger intensive Weise als das Sammeln, Verarbeiten und Aufbewahren von Verkehrs- und Standortdaten. Er prüft zuerst, ob die Aufbewahrungsfrist unter Berücksichtigung der üblichen Dauer einer strafrechtlichen Untersuchung angemessen ist. In Bezug auf den Zugriff auf die gespeicherten Identifizierungsdaten verlangt er, dass die Behörden, die auf die Daten zugreifen können, abschließend in den einschlägigen Vorschriften aufgezählt werden, dass ihr Zugriff auf einer spezifischen und klaren gesetzlichen Grundlage im Strafprozessrecht oder in den Rechtsvorschriften über die Nachrichten- und Sicherheitsdienste beruht und dass er durch einen konkreten Anfangsverdacht gerechtfertigt ist. Sobald die Behörde die abgefragten Identifizierungsdaten nicht mehr benötigt, muss sie diese sofort vernichten. Der Europäische Gerichtshof für Menschenrechte verlangt nicht, dass die betroffene Person über den Zugriff auf ihre Identifizierungsdaten in Kenntnis gesetzt wird. Er verlangt auch nicht, dass für den Zugriff auf bloße Identifizierungsdaten eine vorherige Kontrolle vorgesehen wird; es reicht ein nachträglicher Zugang zu einem unabhängigen Gericht oder einer unabhängigen

Verwaltungsstelle in Verbindung mit den gemeinrechtlichen Rechtsbehelfen, über die der Beschuldigte während eines Strafprozesses verfügt, aus (EuGHMR, 30. Januar 2020, *Breyer gegen Deutschland*, §§ 96-107).

In seinem Entscheid Nr. 57/2021 vom 22. April 2021 hat der Gerichtshof die Artikeln 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 erklärt, weil darin ein allgemeines und unterschiedsloses Sammeln, Verarbeiten und Aufbewahren von sowohl Identifizierungsdaten als auch Verkehr- und Standortdaten vorgesehen war. Der Gerichtshof stellte fest, « 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 [beruhte] und dass es allgemein […] umfassendere Ziele als die Bekämpfung schwerer Kriminalität oder die Gefahr einer schwerwiegenden Beeinträchtigung der öffentlichen Sicherheit [verfolgte] » (B.17). Das angefochtene Gesetz garantierte außerdem weder, dass das Sammeln, Verarbeiten und Aufbewahren von Daten über die elektronische Kommunikation die Ausnahme anstatt der Regel war, noch, dass der Zugriff auf diese Daten klaren und präzisen Regeln unterworfen war, dass sich der Eingriff in das Recht auf Achtung des Privatlebens auf das absolut Notwendige beschränkte und dass jeder Eingriff den objektiven Kriterien genügte, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen (B.18).

B.15.2. Das nunmehr angefochtene Gesetz bezieht sich hingegen lediglich auf die in Artikel 127 des Gesetzes vom 13. Juni 2005 angeführten Daten, anhand deren der Endnutzer eines elektronischen Kommunikationsdienstes, der auf der Grundlage einer Guthabenkarte angeboten wird, identifiziert werden kann. Artikel 12 Absatz 2 des königlichen Erlasses vom 27. November 2016 sieht vor, dass sich diese Identifizierungsdaten je nach der ausgewählten Identifizierungsmethode unterscheiden können, zählt die Identifizierungsdaten, die das betreffende Unternehmen höchstens aufbewahren darf, aber auch abschließend auf:

« 1. Namen und Vornamen,

2. Geschlecht,

3. Staatsangehörigkeit,

4. Geburtsdatum und -ort,

5. Adresse des Wohnsitzes, E-Mail-Adresse und Telefonnummer,

6. Nationalregisternummer,

7. Nummer des Identitätsdokuments, Ausstellungsland bei ausländischen Dokumenten und Gültigkeitsdatum des Dokuments,

8. Referenz des Zahlungsvorgangs gemäß Artikel 17,

9. Verbindung der Guthabenkarte mit dem Produkt, für das der Endnutzer bereits gemäß Artikel 18 identifiziert ist,

10. Foto des Endnutzers, aber nur für andere Dokumente als den belgischen elektronischen Personalausweis ».

Angesichts der teilweisen, in B.9.1 angeführten Nichtigerklärung und der Aufrechterhaltung der Folgen im Sinne der Ausführung in B.9.3 muss der Gesetzgeber die Identifizierungsdaten und -dokumente, die im Rahmen von Artikel 127 des Gesetzes vom 13. Juni 2005 in Betracht kommen können, vor dem im Tenor erwähnten Zeitpunkt gesetzlich festlegen.

B.15.3. Bei diesen personenbezogenen Daten handelt es sich nicht um Verkehrs- und Standortdaten, sondern nur um Daten, die gewöhnlich verwendet werden, um eine Person zu identifizieren. Es ist weder möglich, nur anhand dieser Daten die Ortsveränderungen, die Kommunikationen, die Tätigkeiten oder die sozialen Beziehungen einer Person nachzuverfolgen, noch, ein persönliches Profil zu erstellen, das es erlaubt, genaue Schlüsse auf die sexuelle Orientierung, Überzeugungen und den Gesundheitszustand einer Person zu ziehen. Sie enthalten daher an sich keine sensiblen Informationen über das Privatleben.

Nur dadurch, dass diese Identifizierungsdaten anschließend mit anderen Daten zusammengeführt werden können, können sie dazu beitragen, dass solche sensiblen Informationen über das Privatleben einer Person preisgegeben werden. Diese anderen Daten müssen dann allerdings auf andere Weise gesammelt werden und auch dieses Sammeln muss unter Beachtung der einschlägigen Rechtsvorschriften und der Grundrechte der betroffenen Person erfolgen.

Folglich muss die Vereinbarkeit des angefochtenen Gesetzes mit dem Recht auf Achtung des Privatlebens anhand der in B.14.3 erwähnten Kriterien beurteilt werden.

B.16.1. Die materiellen und prozeduralen Voraussetzungen für das Sammeln, Verarbeiten und Aufbewahren der Identifizierungsdaten von Endnutzern eines elektronischen Kommunikationsnetzwerks im Zusammenhang mit einer Guthabenkarte sind in den Artikeln 126 und 127 des Gesetzes vom 13. Juni 2005 und in den königlichen Erlassen vom 19. September 2013 und vom 27. November 2016 geregelt.

B.16.2. Wie in B.2.1 bis B.2.7 ausgeführt wurde, legt Artikel 127 des Gesetzes vom 13. Juni 2005 fest, welchen Personen in diesem Rahmen Verpflichtungen auferlegt werden, nämlich den Betreibern, den Anbietern, den Vertriebswegen elektronischer Kommunikationsdienste, den Unternehmen, die einen Identifizierungsdienst anbieten, und den Endnutzern selbst. Er regelt auch, wer der zuständige Datenverarbeiter ist, nämlich der Betreiber oder der Anbieter. Er sieht ferner das Prinzip vor, dass alle Endnutzer identifizierbar sein müssen, unabhängig davon, ob sie eine alte oder eine neue Guthabenkarte benutzen, sowie, dass die Identifizierung anhand eines Identifizierungsdokuments mit der Nationalregisternummer erfolgen muss.

Der königliche Erlass vom 27. November 2016 verpflichtet die Endnutzer von Guthabenkarten, sich spätestens bei der Aktivierung dieser Karten beim Betreiber anhand einer der im selben königlichen Erlass vorgesehenen gültigen Identifizierungsmethoden und eines der im königlichen Erlass erwähnten gültigen Identifizierungsdokumente zu identifizieren. Er verpflichtete die Betreiber, alle Endnutzer alter Guthabenkarten vor dem 7. Juni 2017 zu identifizieren, und untersagt ihnen, weiter neue Guthabenkarten zu aktivieren, wenn der Endnutzer noch nicht identifiziert ist. Wenn der Endnutzer sie vom Verlust oder Diebstahl der Guthabenkarte in Kenntnis setzt, müssen sie diese sofort unbrauchbar machen.

In Bezug auf die eigentliche Datenverarbeitung bestimmt der königliche Erlass vom 27. November 2016, dass der Betreiber, der Identifizierungsdiensteanbieter oder der Vertriebsweg elektronischer Kommunikationsdienste den belgischen elektronischen Personalausweis elektronisch lesen oder ihn einscannen, kopieren oder fotografieren, einschließlich des darauf abgebildeten Fotos und seiner Nummer. Der Betreiber muss vor Aktivierung der Guthabenkarte überprüfen, ob der vorgelegte Personalausweis gestohlen oder zu betrügerischen Zwecken verwendet wurde. Er muss ebenso die Identifizierungsmethode, die

verwendet wurde, um den Endnutzer zu identifizieren, während der in Artikel 126 des Gesetzes vom 13. Juni 2005 erwähnten Frist speichern.

B.16.3. Die klagenden Parteien beanstanden nicht, dass diese Regeln klar und präzise sind. Sie machen lediglich geltend, dass der gesetzliche Rahmen in Bezug auf die weitere Aufbewahrung der verarbeiteten Daten seit dem Entscheid Nr. 57/2021 des Gerichtshofs vom 22. April 2021 unklar sei, weil der Gerichtshof in diesem Entscheid die Regeln über die verarbeiteten Daten, die an der Verarbeitung beteiligten Personen, die Bedingungen für die Verarbeitung und deren Ziele sowie die Regeln in Bezug auf das Koordinationsbüro für nicht erklärt habe. Dadurch bestünden keine materiellen und prozeduralen Voraussetzungen mehr, die die Verarbeitung der gespeicherten Identifizierungsdaten oder -dokumente regelten.

B.16.4. Wie in B.8.7.3 ausgeführt wurde, hat der Entscheid Nr. 57/2021 nicht zur Folge, dass es keinen gesetzlichen Rahmen für die Aufbewahrung der gesammelten und verarbeiteten Identifizierungsdaten mehr gibt. Die Nichtigerklärung der Artikel 2 Buchstabe *b)*, 3 bis 11 und 14 des Gesetzes vom 29. Mai 2016 hat nur zur Folge, dass Artikel 126 des Gesetzes vom 13. Juni 2005 jetzt in Bezug auf die Identifizierungsdaten von Nutzern von Guthabenkarten in der Fassung Anwendung findet, die zuletzt durch Artikel 33 des Gesetzes vom 4. Februar 2010 « über die Methoden zum Sammeln von Daten durch die Nachrichten- und Sicherheitsdienste » abgeändert wurde.

B.16.5. Zur Ausführung von Artikel 126 des Gesetzes vom 13. Juni 2005 legt der königliche Erlass vom 19. September 2013 die Voraussetzungen für die Aufbewahrung der gesammelten Daten fest. Die Artikel 3 bis 6 dieses Erlasses bestimmen, welche Daten aufzubewahren sind und wer für die Aufbewahrung verantwortlich ist:

« Art. 3. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs de services de téléphonie fixe accessibles au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° le numéro attribué à l'utilisateur final;

2° les données personnelles de l'utilisateur final;

3° la date de début de l'abonnement ou de l'enregistrement au service;

4° le type de service de téléphonie fixe utilisé ainsi que les services annexes auxquels l'utilisateur final a souscrit;

5° en cas de transfert du numéro de l'utilisateur final auprès d'un autre fournisseur, l'identité du fournisseur qui transfère le numéro et l'identité du fournisseur auquel le numéro est transféré;

6° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs de services de téléphonie fixe accessibles au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identification du numéro de téléphone de l'appelant et de l'appelé;

2° la localisation du point de terminaison du réseau de l'appelant et de l'appelé;

3° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré;

4° la date et l'heure exacte du début et de la fin de l'appel;

5° la description du service de téléphonie utilisé.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi.

Art. 4. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs d'un service de téléphonie mobile accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° le numéro attribué à l'utilisateur final ainsi que l'identité internationale d'abonné mobile (' International Mobile Subscriber Identity ', ' IMSI ');

2° les données personnelles de l'utilisateur final;

3° la date et le lieu de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final;

4° la date et l'heure de la première activation du service, ainsi que l'identifiant cellulaire à partir duquel le service a été activé;

5° les services annexes auxquels l'utilisateur final a souscrit;

6° en cas de transfert de numéro auprès d'un autre opérateur, l'identité de l'opérateur d'origine de l'utilisateur final;

7° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service;

8° le numéro d'identification du terminal mobile de l'utilisateur final (' International Mobile Equipment Identity ', ' IMEI ').

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs d'un service de téléphonie mobile accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identification du numéro de téléphone de l'appelant et de l'appelé;

2° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré;

3° l'identité internationale d'abonné mobile (' International Mobile Subscriber Identity ', ' IMSI ') de l'appelant et de l'appelé;

4° l'identité internationale d'équipement mobile (' International Mobile Equipment Identity ', ' IMEI ') du terminal mobile de l'appelant et de l'appelé;

5° la date et l'heure exacte du début et de la fin de l'appel;

6° la localisation du point de terminaison du réseau au début et à la fin de chaque connexion;

7° les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée;

8° les caractéristiques techniques du service de téléphonie utilisé.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi.

Art. 5. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs de service d'accès à l'internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identifiant de l'utilisateur final;

2° les données personnelles de l'utilisateur final;

3° la date et l'heure de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final;

4° l'adresse IP et le port source de la connexion ayant servi à la création de l'abonnement ou à l'enregistrement de l'utilisateur final;

5° l'identification du point de terminaison du réseau ayant servi à la création de l'abonnement ou de l'inscription en tant qu' utilisateur final;

6° les services annexes auxquels l'utilisateur final a souscrit auprès du prestataire d'accès Internet public concerné;

7° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs de service d'accès à l'internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identifiant de l'utilisateur final;

2° a) l'adresse IP;

b) en cas d'utilisation partagée d'une adresse IP, les ports attribués de l'adresse IP ainsi que la date et l'heure de l'attribution;

3° l'identification et la localisation du point de terminaison du réseau utilisé par l'utilisateur final au début et à la fin d'une connexion;

4° la date et l'heure de l'ouverture et de la fermeture d'une session du service d'accès à l'internet;

5° le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session ou autre unité de temps demandée;

6° les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi .

Art. 6. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs d'un service de courrier électronique par internet accessible au public, les fournisseurs d'un service de téléphonie par internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l’identifiant de l’utilisateur final;

2° les données personnelles de l’utilisateur final;

3° la date et l’heure de la création du compte de courrier électronique ou de téléphonie par internet;

4° l’adresse IP et le port source ayant servi à la création du compte de courrier électronique ou de téléphonie par l’internet;

5° les données relatives au type de paiement, à l’identification du moyen de paiement et à la date du paiement de l’abonnement ou de l’utilisation du service.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs d’un service de courrier électronique par internet accessible au public, les fournisseurs d’un service de téléphonie par internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l’identifiant de l’utilisateur final du compte de courrier électronique ou de téléphonie par internet, ainsi que le numéro ou l’identifiant du destinataire prévu de la communication;

2° le numéro de téléphone attribué à toute communication entrant dans le réseau téléphonique public dans le cadre d’un service téléphonique par internet;

3° a) l’adresse IP et le port source utilisés par l’utilisateur final;

b) l’adresse IP et le port source utilisés par le destinataire;

4° la date et l’heure de l’ouverture et de la fermeture d’une session du service de courrier électronique ou de téléphonie par internet;

5° la date et l’heure de la connexion établie à l’aide du compte de téléphonie par Internet;

6° les caractéristiques techniques du service utilisé.

§ 3. Les données visées au paragraphe 1er sont soumises à l’article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l’article 126, § 3, alinéa 2, de la loi ».

B.16.6. Dieser königliche Erlass sieht jedoch keine Mindest- oder Höchstfristen für die Aufbewahrung der nach Artikel 127 des Gesetzes vom 13. Juni 2005 verarbeiteten Identifizierungsdaten vor. Diese Frist war nämlich in dem durch Entscheid Nr. 57/2021 für nichtig erklärten Artikel 126 § 3 des Gesetzes vom 13. Juni 2005 verankert, der bestimmte:

« 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 ».

Bis zum Inkrafttreten einer neuen Fassung von Artikel 126 des Gesetzes vom 13. Juni 2005 wird der Endnutzer einer Guthabenkarte gleichwohl nicht dem Risiko einer unbegrenzten Aufbewahrung seiner Identifizierungsdaten ausgesetzt. Die zurzeit anwendbare Fassung dieser Bestimmung sieht nämlich eine Höchstspeicherfrist von sechsunddreißig Monaten vor.

Im Übrigen ist dieser Endnutzer durch die Datenschutz-Grundverordnung geschützt, die vom zuständigen Datenverarbeiter neben - und notfalls vorrangig gegenüber - den einschlägigen Bestimmungen des nationalen Rechts zu beachten ist. Nach dem in Artikel 5 Buchstabe e der Datenschutz-Grundverordnung verankerten Grundsatz der Speicherbegrenzung müssen die personenbezogenen Daten vom Datenverarbeiter « in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist ».

Angesichts dieser Bestimmungen kann hingenommen werden, dass bis zum Inkrafttreten eines neuen gesetzlichen Rahmens bezüglich der Vorratsdatenspeicherung die einschlägigen Rechtsvorschriften vorübergehend keine spezifische Speicherfrist vorsehen. Es obliegt in der Zwischenzeit den zuständigen Verwaltungsbehörden und Rechtsprechungsorganen, auf der Grundlage dieser Bestimmungen zu gewährleisten, dass die Identifizierungsdaten der Endnutzer von Guthabenkarten nicht länger aufbewahrt werden, als im Lichte der mit der angefochtenen Identifizierungspflicht verfolgten Ziele notwendig ist.

B.16.7. Diese Ziele sind abschließend in Artikel 127 § 1 des Gesetzes vom 13. Juni 2005 aufgezählt. Es geht um das gute Funktionieren der Notdienste, die strafrechtliche Untersuchung

und das Funktionieren der Nachrichten- und Sicherheitsdienste. Dieses zweite und dritte Ziel stimmen mit den Gründen überein, aus denen der Gerichtshof der Europäischen Union die Aufbewahrung von Identifizierungsdaten erlaubt (EuGH, Große Kammer, 6. Oktober 2020, *La Quadrature du Net u.a.*, C-511/18, C-512/18 und C-520/18, Randnrn. 152 bis 159). Das gute Funktionieren der Notdienste hängt wiederum mit den positiven Verpflichtungen zusammen, die die Behörden im Rahmen der Rechte treffen, die Opfern von Straftaten und Unfällen nach den Artikeln 2, 3, 5 und 8 der Europäischen Menschenrechtskonvention zustehen.

B.16.8.1. Die Rechtsvorschriften zu diesen Diensten regeln außerdem abschließend, welche Behörden auf die gespeicherten Identifizierungsdaten zugreifen können und welche materiellen und prozeduralen Voraussetzungen sie dafür erfüllen müssen.

B.16.8.2. Der Zugriff auf diese Daten im Rahmen einer strafrechtlichen Untersuchung ist in den Artikeln 46*bis*, 88*bis* und 90*ter* bis 90*decies* des Strafprozessgesetzbuches geregelt.

Artikel 46*bis* des Strafprozessgesetzbuches bestimmt:

« § 1. Bei der Ermittlung von Verbrechen und Vergehen kann der Prokurator des Königs durch eine mit Gründen versehene schriftliche Entscheidung auf der Grundlage jeglicher Daten, die in seinem Besitz sind, oder durch einen Zugang zu den Kundendateien der in Absatz 2 erster und zweiter Gedankenstrich erwähnten Akteure Folgendes vornehmen oder vornehmen lassen:

1. die Identifizierung des Teilnehmers oder des gewöhnlichen Nutzers eines in Absatz 2 zweiter Gedankenstrich erwähnten Dienstes oder des benutzten elektronischen Kommunikationsmittels,

2. die Identifizierung der in Absatz 2 zweiter Gedankenstrich erwähnten Dienste, die eine bestimmte Person über einen Festvertrag bezieht oder die gewöhnlich von einer bestimmten Person benutzt werden.

Hierfür kann er erforderlichenfalls unmittelbar oder über einen vom König bestimmten Polizeidienst die Mitwirkung folgender Personen anfordern:

des Betreibers eines elektronischen Kommunikationsnetzes und

jeglicher Person, die auf belgischem Staatsgebiet auf irgendeine Weise einen Dienst bereitstellt oder anbietet, der in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht oder durch den Nutzer dazu ermächtigt werden, über ein elektronisches Kommunikationsnetz Informationen zu erhalten, zu empfangen oder zu verbreiten. Hierzu zählt auch der Anbieter eines elektronischen Kommunikationsdienstes.

Die Begründung spiegelt die Verhältnismäßigkeit unter Berücksichtigung des Privatlebens und die Subsidiarität gegenüber jeder anderen Ermittlungsaufgabe wider.

In Fällen äußerster Dringlichkeit kann der Prokurator des Königs diese Maßnahme mündlich anordnen. Die Entscheidung wird so schnell wie möglich schriftlich bestätigt.

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

§ 2. Die in § 1 Absatz 2 erster und zweiter Gedankenstrich erwähnten Akteure, von denen gefordert wird, die in § 1 erwähnten Daten mitzuteilen, verschaffen dem Prokurator des Königs oder dem Gerichtspolizeioffizier die Daten in Echtzeit oder gegebenenfalls zu dem in der Anforderung bestimmten Zeitpunkt gemäß den vom König auf Vorschlag des Ministers der Justiz und des für das Fernmeldewesen zuständigen Ministers festgelegten Modalitäten.

Der König bestimmt nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und auf Vorschlag des Ministers der Justiz und des für das Fernmeldewesen zuständigen Ministers die technischen Bedingungen für den Zugang zu den in § 1 erwähnten Daten, die für den Prokurator des Königs und für den im selben Paragraphen bestimmten Polizeidienst verfügbar sind.

Jede Person, die aufgrund ihres Amtes Kenntnis von der Maßnahme erlangt oder dabei ihre Mitwirkung gewährt, unterliegt der Schweigepflicht. Jegliche Verletzung der Schweigepflicht wird gemäß Artikel 458 des Strafgesetzbuches geahndet.

Wer sich weigert, Daten mitzuteilen, oder wer Daten nicht in Echtzeit oder gegebenenfalls zu dem in der Anforderung bestimmten Zeitpunkt mitteilt, wird mit einer Geldbuße von sechsundzwanzig bis zu zehntausend EUR bestraft ».

Artikel 88*bis* des Strafprozessgesetzbuches bestimmt:

« § 1. 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 Folgendes 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.

Hierfür kann er erforderlichenfalls unmittelbar oder über einen vom König bestimmten Polizeidienst die Mitwirkung folgender Personen anfordern:

des Betreibers eines elektronischen Kommunikationsnetzes und

jeglicher Person, die auf belgischem Staatsgebiet auf irgendeine Weise einen Dienst bereitstellt oder anbietet, der in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht oder durch den Nutzer dazu ermächtigt werden, über ein elektronisches Kommunikationsnetz Informationen zu erhalten, zu empfangen oder zu verbreiten. Hierzu zählt auch der Anbieter eines elektronischen Kommunikationsdienstes.

In den in Absatz 1 erwähnten Fällen werden für jedes elektronische Kommunikationsmittel, für das die Verbindungsdaten erfasst werden oder die Herkunft oder Bestimmung der elektronischen Nachricht lokalisiert wird, Tag, Uhrzeit, Dauer und, wenn nötig, Ort der elektronischen Nachricht in einem Protokoll angegeben und festgehalten.

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.

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.

Bei Entdeckung auf frischer Tat kann der Prokurator des Königs die Maßnahme für die in Artikel 90*ter* §§ 2, 3 und 4 erwähnten Straftaten anordnen. In diesem Fall muss die Maßnahme binnen vierundzwanzig Stunden vom Untersuchungsrichter bestätigt werden.

Wenn es jedoch die in Artikel 137, 347*bis*, 434 oder 470 des Strafgesetzbuches erwähnte Straftat betrifft, mit Ausnahme der in Artikel 137 § 3 Nr. 6 desselben Gesetzbuches erwähnten Straftat, kann der Prokurator des Königs die Maßnahme anordnen, solange die Situation der Entdeckung auf frischer Tat andauert, ohne dass eine Bestätigung durch den Untersuchungsrichter nötig ist.

Wenn es die in Artikel 137 des Strafgesetzbuches erwähnte Straftat betrifft, mit Ausnahme der in Artikel 137 § 3 Nr. 6 desselben Gesetzbuches erwähnten Straftat, kann der Prokurator des Königs die Maßnahme außerdem binnen zweiundsiebzig Stunden nach Entdeckung dieser Straftat anordnen, ohne dass eine Bestätigung durch den Untersuchungsrichter nötig ist.

Der Prokurator des Königs kann die Maßnahme jedoch auf Ersuchen des Klägers hin anordnen, wenn diese Maßnahme sich als unbedingt notwendig erweist, um eine in Artikel 145 § 3 und § 3*bis* des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation erwähnte Straftat festzustellen.

Im Dringlichkeitsfall kann die Maßnahme mündlich angeordnet werden. Sie muss so schnell wie möglich in der in den Absätzen 4 und 5 vorgesehenen Form bestätigt werden.

§ 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.

§ 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. Diese Personen unterliegen der Schweigepflicht. Jegliche Verletzung der Schweigepflicht wird gemäß Artikel 458 des Strafgesetzbuches geahndet.

§ 4. Die in § 1 Absatz 2 erwähnten Akteure teilen die angeforderten Informationen in Echtzeit oder gegebenenfalls zu dem in der Anforderung bestimmten Zeitpunkt gemäß den vom König auf Vorschlag des Ministers der Justiz und des für das Fernmeldewesen zuständigen Ministers festgelegten Modalitäten mit.

Jede Person, die aufgrund ihres Amtes Kenntnis von der Maßnahme erlangt oder dabei ihre Mitwirkung gewährt, unterliegt der Schweigepflicht. Jegliche Verletzung der Schweigepflicht wird gemäß Artikel 458 des Strafgesetzbuches geahndet.

Wer seine technische Mitwirkung bei den im vorliegenden Artikel erwähnten Anforderungen verweigert oder nicht in Echtzeit oder gegebenenfalls zu dem in der Anforderung bestimmten Zeitpunkt gewährt, wird mit einer Geldbuße von sechsundzwanzig bis zu zehntausend EUR bestraft; die Modalitäten dieser Mitwirkung werden vom König auf Vorschlag des Ministers der Justiz und des für das Fernmeldewesen zuständigen Ministers festgelegt ».

Artikel 90*ter* § 1 des Strafprozeßgesetzbuches bestimmt:

« § 1. Unbeschadet der Anwendung der Artikel 39*bis*, 87, 88, 89*bis* und 90 kann der Untersuchungsrichter der Öffentlichkeit nicht zugängliche Nachrichten oder Daten eines Datenverarbeitungssystems oder eines Teils davon anhand technischer Mittel zu geheimen

Zwecken abfangen, von ihnen Kenntnis nehmen, sie durchsuchen und aufzeichnen oder die Suche in einem Datenverarbeitungssystem oder einem Teil davon ausweiten.

Diese Maßnahme kann nur in Ausnahmefällen angeordnet werden, wenn die Untersuchung es erfordert, wenn schwerwiegende Indizien dafür bestehen, dass sie eine in § 2 erwähnte Straftat betrifft, und wenn die anderen Untersuchungsmittel nicht ausreichen, um die Wahrheit herauszufinden.

Um diese Maßnahme zu ermöglichen, kann der Untersuchungsrichter anordnen, jederzeit auch ohne das Wissen oder ohne die Zustimmung des Bewohners, des Eigentümers oder des Inhabers seiner Rechte oder des Nutzers:

eine Wohnung oder Privatgelände zu betreten oder in ein Datenverarbeitungssystem einzudringen,

jegliche Sicherung der betreffenden Datenverarbeitungssysteme gegebenenfalls mit Hilfe von technischen Mitteln, falschen Signalen, falschen Schlüsseln oder falschen Eigenschaften zeitweilig aufzuheben,

technische Vorrichtungen in die betreffenden Datenverarbeitungssysteme zu installieren im Hinblick auf die Entschlüsselung und die Dekodierung der durch dieses Datenverarbeitungssystem gespeicherten, verarbeiteten oder übermittelten Daten.

Die im vorliegenden Paragraphen erwähnte Maßnahme kann nur angeordnet werden, um Daten zu suchen, die der Wahrheitsfindung dienlich sein können. Sie kann nur entweder gegenüber Personen, die auf der Grundlage genauer Indizien verdächtigt werden, die Straftat begangen zu haben, angeordnet werden oder gegenüber Kommunikationsmitteln oder Datenverarbeitungssystemen, die regelmäßig von einem Verdächtigen benutzt werden, oder gegenüber Orten, wo dieser sich aufzuhalten vermutet wird. Sie kann auch gegenüber Personen angeordnet werden, von denen auf der Grundlage genauer Tatsachen vermutet wird, dass sie in regelmäßigem Kontakt zu einem Verdächtigen stehen ».

B.16.8.3. Der Zugriff auf diese Daten im Rahmen einer Untersuchung durch die Nachrichten- und Sicherheitsdienste ist in Artikel 16/2 § 1 des Gesetzes vom 30. November 1998 geregelt, der festlegt:

« Die Nachrichten- und Sicherheitsdienste können im Interesse der Erfüllung ihrer Aufträge die Mitwirkung eines Betreibers eines elektronischen Kommunikationsnetzes oder eines Anbieters eines elektronischen Kommunikationsdienstes anfordern, um Folgendes vorzunehmen:

1. die Identifizierung des Teilnehmers oder des gewöhnlichen Nutzers eines elektronischen Kommunikationsdienstes oder des benutzten elektronischen Kommunikationsmittels,

2. die Identifizierung der elektronischen Kommunikationsdienste und -mittel, die eine bestimmte Person über einen Festvertrag bezieht oder die gewöhnlich von einer bestimmten Person benutzt werden.

Die Anforderung erfolgt schriftlich durch den Dienstleiter oder seinen Beauftragten. Bei äußerster Dringlichkeit kann der Dienstleiter beziehungsweise sein Beauftragter diese Daten mündlich anfordern. Diese mündliche Anforderung wird binnen vierundzwanzig Stunden durch eine schriftliche Anforderung bestätigt.

Jeder Betreiber eines elektronischen Kommunikationsnetzes und jeder Anbieter eines elektronischen Kommunikationsdienstes, dessen Mitwirkung angefordert wird, verschafft dem Dienstleiter beziehungsweise seinem Beauftragten die angeforderten Daten innerhalb einer Frist und gemäß den Modalitäten, die durch Königlichen Erlass auf Vorschlag des Ministers der Justiz, des Ministers der Landesverteidigung und des für elektronische Kommunikation zuständigen Ministers festzulegen sind.

Der Dienstleiter beziehungsweise sein Beauftragter kann, unter Einhaltung der Verhältnismäßigkeits- und Subsidiaritätsprinzipien und unter der Bedingung, dass die Abfrage aufgezeichnet wird, die erwähnten Daten zudem durch einen Zugriff auf die Dateien der Kunden des Betreibers beziehungsweise des Anbieters des Dienstes erhalten. Der König legt auf Vorschlag des Ministers der Justiz, des Ministers der Landesverteidigung und des für elektronische Kommunikation zuständigen Ministers die technischen Bedingungen fest, unter denen dieser Zugriff möglich ist ».

B.16.8.4. Der Zugriff auf diese Daten durch die Notdienste ist in Artikel 107 § 2 des Gesetzes vom 13. Juni 2005 geregelt, der festlegt:

« Betreiber, die von einem Notruf an einen Hilfsdienst, der vor Ort Hilfe leistet, betroffen sind, liefern, wenn nötig in gegenseitiger Abstimmung, den Leitstellen dieses Hilfsdienstes unmittelbar nach Eingang des Anrufs und kostenlos die Identifizierungsdaten des Anrufers.

Diese Verpflichtung gilt ebenfalls, wenn die Leitstellen der Hilfsdienste, die vor Ort Hilfe leisten, von einer Organisation betrieben werden, die von den öffentlichen Behörden mit dieser Aufgabe betraut worden ist.

Investitions- und Betriebskosten in Bezug auf Datenbanken mit Identifizierungsdaten des Anrufers und Anschlussleitungen, die Hilfsdienste benutzen, um diese Datenbanken abzufragen, gehen zu Lasten der Betreiber.

Falls ein Betreiber Teilnehmern seine eigenen kommerziellen Dienste für die Bereitstellung von Standortdaten anbietet, dann müssen sowohl die Präzision der Standortdaten, die Teil der Identifizierung des Anrufers bei einem Notruf sind und die gemäß vorliegendem Paragraphen an Hilfsdienste, die vor Ort Hilfe leisten, geliefert werden müssen, als auch die Geschwindigkeit, mit der sie dem betreffenden Hilfsdienst übertragen werden, mindestens der besten von diesem Betreiber kommerziell angebotenen Qualität entsprechen. Das Institut kann in Absprache mit den betreffenden Hilfsdiensten Kriterien für die Genauigkeit und Zuverlässigkeit der Angaben zum Anruferstandort festlegen.

Identifizierungsdaten des Anrufers können von Hilfsdiensten, die vor Ort Hilfe leisten, oder von der Organisation, die von den öffentlichen Behörden mit dem Betreiben der Leitstellen von Hilfsdiensten betraut worden ist, aufgrund administrativer und technischer Maßnahmen,

die vom Minister nach Stellungnahme des Instituts und des Ausschusses für den Schutz des Privatlebens gebilligt worden sind, verwendet werden, um böswilligen Anrufen oder dem Missbrauch von Notrufnummern entgegenzuwirken. Diese Maßnahmen dürfen allerdings nicht dazu führen, dass die Notrufnummer des betreffenden Hilfsdienstes von einem bestimmten Anschluss aus für einen ununterbrochenen Zeitraum von mehr als vierundzwanzig Stunden nicht zugänglich ist.

Die Leitstellen von Hilfsdiensten, die vor Ort Hilfe leisten, erhalten von den betreffenden Betreibern kostenlos die in ihrem Netz verfügbaren Identifizierungsdaten des Anrufers, um Notrufe bearbeiten und böswilligen Anrufen entgegenwirken zu können, selbst wenn der betreffende Nutzer die Unterdrückung der Anzeige seiner Identifizierungsdaten veranlasst hat. Das Format der bereitgestellten Identifizierungsdaten des Anrufers muss dem anwendbaren ETSI-Standard entsprechen und wird vom Institut in Absprache mit den Hilfsdiensten und den Betreibern bestimmt.

Identifizierungsdaten des Anrufers können von Hilfsdiensten, die Fernhilfe leisten, aufgrund administrativer und technischer Maßnahmen, die vom Minister nach Stellungnahme des Instituts und des Ausschusses für den Schutz des Privatlebens gebilligt worden sind, verwendet werden, um böswilligen Anrufen entgegenzuwirken. Diese Maßnahmen dürfen allerdings nicht dazu führen, dass die Notrufnummer des betreffenden Hilfsdienstes von einem bestimmten Anschluss aus für einen ununterbrochenen Zeitraum von mehr als vierundzwanzig Stunden nicht zugänglich ist ».

B.16.8.5. Diese Bestimmungen regeln die materiellen und prozeduralen Voraussetzungen, unter denen diese Behörden auf die nach Artikel 127 des Gesetzes vom 13. Juni 2005 verarbeiteten Identifizierungsdaten zugreifen können, klar und präzise.

Wenn sie auf diese Daten zugreifen, müssen diese Behörden nicht nur die in B.16.8.2 bis B.16.8.4 erwähnten Regeln beachten, sondern auch die Grundrechte des Endnutzers, wie sie unter anderem in der Datenschutz-Grundverordnung, den Artikeln 6 und 8 der Europäischen Menschenrechtskonvention und den Artikeln 7, 8 und 47 der Charta gewährleistet sind.

B.16.8.6. In diesem Zusammenhang verweisen die klagenden Parteien auf das Urteil der Großen Kammer des Gerichtshofs der Europäischen Union vom 2. März 2021 in Sachen *Prokuratuur* (C-746/18, Randnrn. 50 bis 56), in dem der Gerichtshof der Europäischen Union nach ihrer Ansicht verlangt, dass eine unabhängige Verwaltungsstelle oder ein Gericht jeden Antrag auf Zugriff vorher anhand der einschlägigen nationalen Regeln und der Grundrechte prüfe, und in dem er nach ihrer Auffassung präzisiert, dass bei der Staatsanwaltschaft, die das Ermittlungsverfahren leite und gegebenenfalls die öffentliche Klage vertrete, die erforderliche Unabhängigkeit nicht vorliege, um diese Prüfung vornehmen zu können.

Dieses Urteil bezog sich allerdings auf einen Antrag der Staatsanwaltschaft auf Zugriff auf Verkehrs- und Standortdaten. Wie in B.14.3 ausgeführt wurde, verlangen der Gerichtshof der Europäischen Union und der Europäische Gerichtshof für Menschenrechte demgegenüber keine vorherige Prüfung eines Antrags auf Zugriff auf Identifizierungsdaten durch ein Gericht oder eine Verwaltungsstelle. Folglich steht das Recht auf Achtung des Privatlebens einem Antrag auf Zugriff auf solche Daten, der von der Staatsanwaltschaft gestellt wird, nicht entgegen.

B.16.8.7. Gleichwohl muss der Antrag auf Zugriff auf die nach Artikel 127 des Gesetzes vom 13. Juni 2005 verarbeiteten Identifizierungsdaten immer *in concreto* begründet werden, indem der Zusammenhang zwischen diesen Daten und den objektiven Elementen nachgewiesen wird, die den konkreten Anfangsverdacht hinsichtlich des betroffenen Endnutzers wegen einer spezifischen Straftat untermauern. Ebenso muss begründet werden, dass nicht mehr Daten als im Lichte der laufenden Ermittlungen absolut notwendig abgefragt werden. Eine solche Begründung darf weder Standardformulierungen noch Stilmittel zum Gegenstand haben.

B.16.9.1. Das Gesetz vom 13. Juni 2005 und die königlichen Erlasse vom 19. September 2013 und vom 26. November 2016 enthalten Garantien gegen Missbrauch im Rahmen der Sammlung, Verarbeitung und Aufbewahrung der Identifizierungsdaten.

Artikel 127 § 1 des Gesetzes vom 13. Juni 2005 legt fest, dass der Vertriebsweg elektronischer Kommunikationsdienste die gesammelten Identifizierungsdaten und -dokumente an den Betreiber übermittelt, ohne selbst Kopien zu speichern. Wenn eine unmittelbare Eingabe dieser Daten in das Computersystem nicht möglich ist, kann der Vertriebsweg eine zeitlich befristete Kopie des Identifizierungsdokuments machen, die er spätestens zum Zeitpunkt der Aktivierung der Guthabenkarte vernichtet.

Nach Artikel 11 § 1 des königlichen Erlasses vom 27. November 2016 muss das betreffende Unternehmen systematisch überprüfen, dass ein vorgelegter Personalausweis nicht gestohlen oder zu betrügerischen Zwecken verwendet wurde. Nach Artikel 12 Absatz 3 desselben königlichen Erlasses muss das betreffende Unternehmen oder der Identifizierungsdiensteanbieter die Kopie des Fotos auf dem elektronischen Personalausweis spätestens vor Aktivierung der Guthabenkarte vernichten.

Nach Artikel 8 des königlichen Erlasses vom 19. September 2013 muss jeder Anbieter unter den Mitgliedern des Koordinationsbüros Justiz einen Datenschutzbeauftragten ernennen, der im Rahmen des Schutzes personenbezogener Daten vollkommen unabhängig gegenüber diesem Anbieter handelt und Zugang zu allen relevanten Daten und Räumen dieses Anbieters hat. Er muss darüber wachen, dass alle Verarbeitungen die in Artikel 126 des Gesetzes vom 13. Juni 2005 erwähnten Ziele verfolgen, dass nur die nach dieser Bestimmung und dem königlichen Erlass vom 19. September 2013 ermächtigten Personen auf die Daten zugreifen können und dass alle Maßnahmen zum Schutz der in Artikel 126 des Gesetzes vom 13. Juni 2005 genannten Daten eingehalten werden.

B.16.9.2. Auf dem Gebiet des Zugriffs auf die gespeicherten Daten legt Artikel 9 des königlichen Erlasses vom 19. September 2013 fest, dass jeder Anbieter jährlich vor dem 1. März dem Belgischen Institut für Post- und Fernmeldewesen mitteilt, wie oft im vorangegangenen Kalenderjahr Daten an die zuständigen Behörden übermittelt wurden, wie viel Zeit zwischen der Verarbeitung und dem Abfragen der Daten verstrichen ist und in welchen Fällen den Anträgen auf Übermittlung von Daten nicht entsprochen werden konnte. Dieses Institut stellt diese Informationen jährlich dem Minister der Justiz zur Verfügung.

Nach Artikel 90*decies* des Strafprozessgesetzbuches muss der Minister der Justiz außerdem dem Parlament jährlich Bericht über die Anwendung von unter anderem den Artikeln 46*bis*, 88*bis* und 90*ter* bis 90*novies* desselben Gesetzbuches erstatten. Diese Inkenntnissetzung betrifft die Zahl der Untersuchungen, die Anlass zu den in diesen Artikeln erwähnten Maßnahmen gegeben haben, die Dauer dieser Maßnahmen, die Zahl der betroffenen Personen und die erzielten Ergebnisse.

Nach Artikel 21 des Gesetzes vom 30. November 1998 werden die personenbezogenen Daten, die im Rahmen dieses Gesetzes verarbeitet werden, durch die Nachrichten- und Sicherheitsdienste nicht länger aufbewahrt, als es für die Zwecke, derentwegen sie gespeichert werden, notwendig ist.

Der vom Gerichtshof in seinem Entscheid Nr. 57/2021 für nichtig erklärte Artikel 126 §§ 4 bis 6 des Gesetzes vom 13. Juni 2005 sah noch weitere Garantien gegen Missbrauch vor:

« § 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 ».

Es obliegt dem Gesetzgeber, wenn er einen neuen gesetzlichen Rahmen für die Vorratsdatenspeicherung schafft, der die im Entscheid Nr. 57/2021 erwähnten Kriterien erfüllt, darin erneut Garantien gegen Missbrauch aufzunehmen. Bis zu diesem Zeitpunkt darf - angesichts der anderen erwähnten Garantien gegen Missbrauch - das Fehlen einer solchen Bestimmung, die sich nur auf den Zugriff auf die gespeicherten personenbezogenen Daten bezieht, nicht zu einer Nichtigerklärung des angefochtenen Gesetzes führen, das nämlich nur die ursprüngliche Sammlung, Verarbeitung und Aufbewahrung der Identifizierungsdaten von Nutzern einer Guthabenkarte betrifft.

B.16.10. Artikel 127 des Gesetzes vom 13. Juni 2005 sieht keine spezifische richterliche Kontrolle bezüglich der Verarbeitung der nach Artikel 127 des Gesetzes vom 13. Juni 2005 verarbeiteten Identifizierungsdaten vor. Wie in B.14.3 ausgeführt wurde, reichen im Rahmen der Verarbeitung bloßer Identifizierungsdaten und des Zugriffs auf diese allerdings die gemeinrechtlichen Rechtsbehelfe aus (EuGHMR, 30. Januar 2020, *Breyer gegen Deutschland*, § 106).

Im Rahmen eines Strafverfahrens verfügt der Angeklagte in diesem Zusammenhang über das Recht, vor den Untersuchungsgerichten oder dem erkennenden Gericht die Nichtigkeit einer Untersuchungshandlung geltend zu machen, die sein Recht auf Achtung des Privatlebens oder sein Reicht auf ein faires Verfahren verletzt.

Im Rahmen der Arbeit der Nachrichten- und Sicherheitsdienste verfügt die betroffene Person nach Artikel 79 des Gesetzes vom 30. Juli 2018 « über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten » über das Recht, beim Ständigen Ausschuss N zu beantragen, dass seine unrichtigen personenbezogenen Daten berichtigt oder entfernt werden und dass die Einhaltung der einschlägigen Bestimmungen überprüft wird.

Ebenso verfügt jeder Endnutzer einer Guthabenkarte, dessen Identifizierungsdaten in Widerspruch zu Artikel 127 des Gesetzes vom 13. Juni 2005 und dem königlichen Erlass vom 27. November 2016 verarbeitet wurden, über eine gemeinrechtliche Haftpflichtklage gegen die Person, die gegen diese Gesetzesbestimmung verstoßen hat.

Schließlich kann die betroffene Person im Falle einer unrechtmäßigen Verarbeitung ihrer personenbezogenen Daten nach Artikel 58 des Gesetzes vom 3. Dezember 2017 « zur Schaffung der Datenschutzbehörde » kostenlos eine Beschwerde bei der Datenschutzbehörde einreichen.

B.16.11.1. Die drei legitimen Ziele, die der Gesetzgeber mit Artikel 127 des Gesetzes vom 13. Juni 2005 verfolgt, nämlich das Ziel des guten Funktionierens der Notdienste, das Ziel der Feststellung, Verfolgung und Bestrafung von Straftaten und das Ziel der Informationsgewinnung durch die Nachrichten- und Sicherheitsdienste hängen alle mit den positiven Verpflichtungen zusammen, die den Staat in Bezug auf das Recht auf Leben, das Verbot unmenschlicher und erniedrigender Behandlung und das Recht auf Freiheit und Sicherheit der gesamten Bevölkerung treffen.

B.16.11.2. Eine Maßnahme, die die Identifizierbarkeit aller Endnutzer einer Guthabenkarte vorsieht, ist für die Verwirklichung dieser Ziele sachdienlich.

Die Möglichkeit, eine Guthabenkarte zu veräußern, und die Möglichkeit, dass sie gestohlen wird, reichen nicht aus, um diesbezüglich zu einem anderen Schluss zu gelangen. Artikel 127 § 1 Absatz 3 des Gesetzes vom 13. Juni 2005 legt deshalb im Übrigen fest, dass die identifizierte Person als Nutzer des elektronischen Kommunikationsdienstes gilt. Diese Bestimmung soll diese Person dazu anhalten, Vorsicht bei der Nutzung ihrer Guthabenkarte durch Dritte walten zu lassen. Artikel 5 des königlichen Erlasses vom 27. November 2016 beschränkt außerdem die Möglichkeit, eine Guthabenkarte Dritten zu überlassen: Mit

Ausnahme der Konstellation, dass die Guthabenkarte einem engen Familienmitglied überlassen wird (Artikel 5 Nrn. 1 bis 3), ist eine Überlassung nur möglich, wenn sich dieser Dritte zuvor beim betreffenden Unternehmen identifiziert (Artikel 5 Nr. 4), wenn eine juristische Person, die eine Guthabenkarte einer natürlichen Person überlässt, die Dienste für sie erbringt, darüber eine aktualisierte Liste aufbewahrt (Artikel 5 Nr. 5), oder wenn die Guthabenkarte für Rechnung der Nachrichten- und Sicherheitsdienste, der Polizeidienste oder bestimmter durch königlichen Erlass festgelegter öffentlicher Behörden gekauft wird (Artikel 5 Nr. 6). Artikel 6 desselben königlichen Erlasses verpflichtet den Endnutzer, das betreffende Unternehmen binnen vierundzwanzig Stunden vom Diebstahl oder Verlust der Guthabenkarte in Kenntnis zu setzen.

Auch das Vorhandensein anderer Kommunikationstechniken hindert den Gesetzgeber nicht daran, die Anonymität bei Guthabenkarten abzuschaffen, wenn er feststellt, dass diese Karten insbesondere in terroristischen und kriminellen Milieus verwendet werden und dass diese Anonymität ein unüberwindbares Problem für die Justizbehörden und die Nachrichten- und Sicherheitsdienste darstellt. Wenn die angefochtene Bestimmung zur Folge hat, dass terroristische und kriminelle Organisationen auf fortschrittlichere Techniken umsteigen, ist dies im Übrigen eher ein Beweis dafür, dass die angefochtene Maßnahme sachdienlich ist. Es ist dann Aufgabe des Gesetzgebers im Hinblick auf die gleichen Ziele auch die Nutzung dieser Techniken zu regeln.

B.16.11.3. Angesichts der in B.16.1 bis B.16.9.3 erwähnten Garantien ist die Identifizierbarkeit des Endnutzers einer Guthabenkarte, die als Maßnahme mit einer geringen Sensibilität hinsichtlich des Privatlebens einzustufen ist, im Lichte dieser Ziele auch verhältnismäßig. Der Umstand, dass sich diese Maßnahme auf alle Endnutzer von Guthabenkarten bezieht, auch wenn ihnen kein kriminelles Verhalten zur Last gelegt werden kann, ändert daran nichts, da eine Maßnahme der Identifizierbarkeit nur funktionieren kann, sofern jeder identifiziert werden kann, sobald das erforderlich ist.

B.16.11.4. Schließlich konnte es den Nutzern von Guthabenkarten nicht entgangen sein, dass die Anonymität bei diesen Karten irgendwann abgeschafft werden würde. Wie in B.2.1 bis B.2.7 ausgeführt wurde, wurde diese Anonymität nämlich immer als zeitlich befristete Ausnahme von der Regel angesehen, dass alle Endnutzer elektronischer Kommunikationsnetzwerke identifizierbar sein müssen.

B.16.12. Vorbehaltlich der in B.8.7.3, B.16.6, B.16.8.5 und B.16.8.7 erwähnten Auslegungen ist der erste Teil des zweiten Klagegrunds unbegründet.

In Bezug auf den zweiten Teil des zweiten Klagegrunds

B.17. Im zweiten Teil des zweiten Klagegrundes führen die klagenden Parteien an, dass das angefochtene Gesetz gegen die Niederlassungsfreiheit und den freien Dienstleistungsverkehr verstoße.

B.18. Jede nationale Maßnahme, die zur Folge haben kann, dass der freie Dienstleistungsverkehr für Unternehmen aus einem anderen Mitgliedstaat der Europäischen Union erschwert oder weniger attraktiv wird, stellt eine Einschränkung des freien Dienstleistungsverkehrs dar. Darüber hinaus sieht Artikel 56 des Vertrags über die Arbeitsweise der Europäischen Union nicht nur Rechte zugunsten des Diensteanbieters selbst vor, sondern auch zugunsten des Dienstleistungsempfängers.

Eine solche Beschränkung kann jedoch « durch zwingende Gründe des Allgemeininteresses gerechtfertigt sein, sofern sie geeignet [ist], die Erreichung des verfolgten Ziels zu gewährleisten, und nicht über das [hinausgeht], was zur Erreichung dieses Ziels erforderlich ist, d.h., wenn es keine weniger einschränkenden Maßnahmen gibt, die es ermöglichen, dieses Ziel ebenso wirksam zu erreichen » (EuGH, 11. Februar 2021, C-407/19 und C-471/19, *Katoen Natie Bulk Terminals NV u.a.*, Randnrn. 59 bis 61).

B.19.1. Ohne dass es notwendig wäre, zu prüfen, ob das angefochtene Gesetz die Niederlassungsfreiheit oder den freien Dienstleistungsverkehr einschränkt, reicht es aus, festzustellen, dass dies durch zwingende Gründe des Allgemeininteresses gerechtfertigt ist, nämlich das gute Funktionieren der Notdienste, die wirksame Feststellung, Verfolgung und Bestrafung von Straftaten und die Vorbeugung terroristischer Handlungen, indem sichergestellt wird, dass die Nachrichten- und Sicherheitsdienste potenzielle Gefahren mit der Identität von Personen, deren Kommunikation abgefangen wird, in Verbindung bringen können.

B.19.2. Wie in B.16.11.2 ausgeführt wurde, ist das angefochtene Gesetz für die Verwirklichung dieser Ziele geeignet. Außerdem geht es nicht über das hinaus, was zur Erreichung dieser Ziele notwendig ist. Eine Maßnahme, die sicherstellen soll, dass die Endnutzer eines belgischen elektronischen Kommunikationsnetzwerks identifizierbar sind, kann nämlich nur dann von Nutzen sein, wenn sie ohne Ausnahme auf alle Endnutzer dieses Netzwerkes Anwendung findet, unabhängig davon, ob sie über einen Festvertrag oder eine Guthabenkarte telefonieren, unabhängig davon, ob diese Karte bereits vor Inkrafttreten des angefochtenen Gesetzes gekauft wurde, und unabhängig davon, ob es um eine Karte geht, die von einem in Belgien oder in einem anderen Mitgliedstaat der Europäischen Union niedergelassenen Unternehmen bereitgestellt wird.

Der Ausschluss von Guthabenkarten, die von in einem anderen Mitgliedstaat niedergelassenen Unternehmen bereitgestellt werden, vom Anwendungsbereich von Artikel 127 des Gesetzes vom 13. Juni 2005 würde die Identifizierbarkeit in der Praxis unmöglich machen, da sich insbesondere Personen mit bösen Absichten ihr einfach entziehen könnten, indem sie eine Guthabenkarte von einem in einem anderen Mitgliedstaat niedergelassenen Unternehmen erwerben.

B.19.3. Der zweite Teil des zweiten Klagegrunds ist unbegründet.

In Bezug auf den dritten Teil des zweiten Klagegrunds

B.20. Im dritten Teil des zweiten Klagegrundes führen die klagenden Parteien an, dass das angefochtene Gesetz gegen die Freiheit der Meinungsäußerung verstoße, da die Identifizierbarkeit von Endnutzern einer Guthabenkarte diese davon abhalte, Politiker und Journalisten zu informieren, und somit die Freiheit, Informationen und Ideen zu empfangen, und die Geheimhaltung journalistischer Quellen auf unverhältnismäßige Weise einschränke.

B.21.1. Die Freiheit der Meinungsäußerung ist eine der Säulen einer demokratischen Gesellschaft. Sie gilt nicht nur für die « Information » oder die « Ideen », die positiv aufgenommen oder als harmlos oder neutral angesehen werden, sondern auch für diejenigen, die den Staat oder irgendeine Bevölkerungsgruppe « schockieren, verunsichern oder verletzen ». Dies erfordern der Pluralismus, die Toleranz und der Geist der Offenheit, ohne die

keine demokratische Gesellschaft bestehen kann (EuGHMR, 7. Dezember 1976, *Handyside gegen Vereinigtes Königreich*, § 49, 23. September 1998, *Lehideux und Isorni gegen Frankreich*, § 55; 28. September 1999, *Öztürk gegen Türkei*, § 64; Große Kammer, 13. Juli 2012, *Mouvement raëlien suisse gegen Schweiz*, § 48).

Dennoch bringt die Ausübung der Freiheit der Meinungsäußerung, wie aus der Formulierung von Artikel 10 Absatz 2 der Europäischen Menschenrechtskonvention ersichtlich ist, gewisse Pflichten und Verantwortungen mit sich (EuGHMR, 4. Dezember 2003, *Gündüz* gegen Türkei, § 37), unter anderem die grundsätzliche Pflicht, gewisse Grenzen, « die insbesondere dem Schutz des guten Rufes und der Rechte anderer dienen » nicht zu überschreiten (EuGHMR, 24. Februar 1997, *De Haes und Gijsels gegen Belgien*, § 37; 21. Januar 1999, *Fressoz und Roire gegen Frankreich*, § 45; 15. Juli 2003, *Ernst u.a. gegen Belgien*, § 92). Der Freiheit der Meinungsäußerung können aufgrund von Artikel 10 Absatz 2 der Europäischen Menschenrechtskonvention unter bestimmten Bedingungen Formalitäten, Bedingungen, Einschränkungen oder Sanktionen auferlegt werden, unter anderem im Hinblick auf den Schutz des guten Rufes oder der Rechte anderer. Die Ausnahmen, mit denen sie einhergehen, sind jedoch « in engem Sinne auszulegen und die Notwendigkeit, sie einzuschränken, muss auf überzeugende Weise bewiesen werden » (EuGHMR, Große Kammer, 20. Oktober 2015, *Pentikäinen gegen Finnland*, § 87).

Artikel 19 der Verfassung verbietet es, dass der Freiheit der Meinungsäußerung präventive Einschränkungen auferlegt werden, jedoch nicht, dass Straftaten, die anlässlich der Inanspruchnahme dieser Freiheit begangen werden, bestraft werden.

B.21.2. Das Recht auf Geheimhaltung der journalistischen Quellen muss also gewährleistet werden, nicht so sehr zum Schutz der Interessen der Journalisten als Berufsgruppe, sondern vielmehr, um es der Presse zu ermöglichen, ihre Rolle als « Wachhund » zu spielen und die Öffentlichkeit über Fragen von allgemeinem Interesse zu informieren. Aus diesem Grund ist das Recht Bestandteil der Freiheit der Meinungsäußerung und der Pressefreiheit.

B.21.3. Nach Auffassung des Europäischen Gerichtshofes kann « eine Übermittlung von Verkehrs- und Standortdaten an Behörden zu Sicherheitszwecken […] die Nutzer […] von der Ausübung ihrer durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung

abhalten […]. 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 » (EuGH, Große Kammer, 6. Oktober 2020, C-623/17, *Privacy International*, Randnr. 72; siehe im selben Sinne EuGH, Große Kammer, 8. April 2014, C-293/12 und C-594/12, *Digital Rights Ireland u.a.*, Randnr. 28; 21. Dezember 2016, C-203/15 und C-698/15, *Tele2 Sverige u.a.*, Randnr. 101; 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, Randnr. 118).

B.22. Artikel 127 des Gesetzes vom 13. Juni 2005 bezieht sich ausschließlich auf die Aufbewahrung und Verarbeitung der Identifizierungsdaten im Sinne von Artikel 12 des königlichen Erlasses vom 27. November 2016. Solche Daten gewähren an sich keinen Einblick in die persönlichen Standpunkte der identifizierten Person. Auch die Verkehrs- und Standortdaten, mit denen sie zusammengeführt werden könnten, stellen an sich keine Meinungsäußerung dar.

Erst wenn diese Daten auch mit dem Inhalt geführter Kommunikation verknüpft werden würden und die diesbezügliche Auswertung Anlass zu weiteren Maßnahmen wie dem Führen einer Untersuchung durch die Nachrichten- und Sicherheitsdienste oder der Einleitung einer strafrechtlichen Untersuchung geben würde, kann das eine Einschränkung der Freiheit der Meinungsäußerung, der Freiheit, Informationen zu gewinnen, der Pressefreiheit oder des Quellengeheimnisses zur Folge haben.

Wie in B.15.3 ausgeführt wurde, muss eine Verknüpfung von Identifizierungsdaten mit anderen Metadaten oder dem Inhalt einer Kommunikation allerdings auf einer klaren und unzweideutigen Gesetzesbestimmung beruhen, die diesbezüglichen materiellen und prozeduralen Voraussetzungen erfüllen und im Einklang mit den Grundrechten der betroffenen Person vorgenommen werden.

Ein solcher mittelbarer Zusammenhang zwischen der angefochtenen Abschaffung der Anonymität bei Guthabenkarten und dem Inhalt geführter Kommunikation reicht nicht aus, um

das angefochtene Gesetz als einschränkende Maßnahme hinsichtlich der Freiheit der Meinungsäußerung einzustufen. Das bloße Sammeln von Identifizierungsdaten aller Endnutzer eines elektronischen Kommunikationsnetzwerks rechtfertigt in einem demokratischen Rechtsstaat nicht die Befürchtung, dass der Staat alle über dieses Netzwerk geführten Kommunikationen überwachen wird. Das angefochtene Gesetz kann folglich an sich nicht dazu führen, dass Personen davon abgehalten werden, ihre Meinung zu äußern oder Informationen mit Journalisten oder Politikern zu teilen.

Der dritte Teil des zweiten Klagegrunds ist unbegründet.

In Bezug auf den dritten Klagegrund

B.23. Im dritten Klagegrund führen die klagenden Parteien an, dass Artikel 2 Nr. 1 Buchstabe *c)* des angefochtenen Gesetzes gegen die Artikel 10, 11, 12 und 14 der Verfassung in Verbindung mit den Artikeln 6 und 7 der Europäischen Menschenrechtskonvention, mit den Artikeln 48, 49 und 52 der Charta, mit dem Recht auf ein faires Verfahren, dem Grundsatz der Unschuldsvermutung und dem Legalitätsprinzip in Strafsachen verstoße, weil die in dieser Bestimmung geregelte Vermutung, dass die Kommunikation dem identifizierten Endnutzer der Guthabenkarte zuzuordnen sei, zur Folge haben könne, dass ihm Taten zur Last gelegt würden, die er nicht begangen habe.

B.24.1. Artikel 12 der Verfassung bestimmt:

« Die Freiheit der Person ist gewährleistet.

Niemand darf verfolgt werden, es sei denn in den durch Gesetz bestimmten Fällen und in der dort vorgeschriebenen Form.

Außer bei Entdeckung auf frischer Tat darf jemand nur festgenommen werden aufgrund einer mit Gründen versehenen richterlichen Anordnung, die spätestens binnen achtundvierzig Stunden ab der Freiheitsentziehung zugestellt werden muss und nur eine Untersuchungsinhaftierung zur Folge haben darf ».

Artikel 14 bestimmt:

« Eine Strafe darf nur aufgrund des Gesetzes eingeführt oder angewandt werden ».

Artikel 7 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Niemand darf wegen einer Handlung oder Unterlassung verurteilt werden, die zur Zeit ihrer Begehung nach innerstaatlichem oder internationalem Recht nicht strafbar war. Es darf auch keine schwerere als die zur Zeit der Begehung angedrohte Strafe verhängt werden.

(2) Dieser Artikel schließt nicht aus, dass jemand wegen einer Handlung oder Unterlassung verurteilt oder bestraft wird, die zur Zeit ihrer Begehung nach den von den zivilisierten Völkern anerkannten allgemeinen Rechtsgrundsätzen strafbar war ».

Artikel 49 der Charta bestimmt:

« (1) Niemand darf wegen einer Handlung oder Unterlassung verurteilt werden, die zur Zeit ihrer Begehung nach innerstaatlichem oder internationalem Recht nicht strafbar war. Es darf auch keine schwerere Strafe als die zur Zeit der Begehung angedrohte Strafe verhängt werden. Wird nach Begehung einer Straftat durch Gesetz eine mildere Strafe eingeführt, so ist diese zu verhängen.

(2) Dieser Artikel schließt nicht aus, dass eine Person wegen einer Handlung oder Unterlassung verurteilt oder bestraft wird, die zur Zeit ihrer Begehung nach den allgemeinen, von der Gesamtheit der Nationen anerkannten Grundsätzen strafbar war.

(3) Das Strafmaß darf gegenüber der Straftat nicht unverhältnismäßig sein ».

B.24.2. Indem er der gesetzgebenden Gewalt die Befugnis verleiht, die Fälle zu bestimmen, in denen eine Strafverfolgung möglich ist, gewährleistet Artikel 12 Absatz 2 der Verfassung jedem Rechtsunterworfenen, dass kein Verhalten strafbar ist, außer aufgrund von Regeln, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

Außerdem beruht das Legalitätsprinzip in Strafsachen, das sich aus der vorerwähnten Verfassungsbestimmung ergibt, auf der Überlegung, dass das Strafgesetz so formuliert sein muss, dass jeder zu dem Augenblick, wo er ein Verhalten annimmt, wissen kann, ob dieses Verhalten strafbar ist oder nicht. Es erfordert es, dass der Gesetzgeber in einer ausreichend präzisen, klaren und Rechtssicherheit bietenden Formulierung angibt, welche Handlungen unter Strafe gestellt werden, sodass einerseits derjenige, der ein Verhalten annimmt, vorher auf hinlängliche Weise beurteilen kann, welche strafrechtlichen Folgen dieses Verhalten haben wird, und andererseits dem Richter keine allzu große Ermessensbefugnis überlassen wird.

Das Legalitätsprinzip in Strafsachen verhindert jedoch nicht, dass das Gesetz dem Richter eine Ermessensbefugnis gewährt. Man muss nämlich der allgemeinen Beschaffenheit der Gesetze, der Verschiedenartigkeit der Situationen, auf die sie Anwendung finden, und der Entwicklung der durch sie geahndeten Verhaltensweisen Rechnung tragen.

Die Bedingung, dass eine Straftat durch das Gesetz klar definiert sein muss, ist erfüllt, wenn der Rechtsunterworfene anhand der Formulierung der relevanten Bestimmung und gegebenenfalls mit Hilfe ihrer Auslegung durch die Rechtsprechungsorgane wissen kann, durch welche Handlungen und Unterlassungen er strafrechtlich haftbar wird.

Erst durch die Prüfung einer spezifischen Strafbestimmung ist es möglich, unter Berücksichtigung der jeweiligen Elemente der dadurch zu ahndenden Straftaten festzustellen, ob die vom Gesetzgeber verwendete allgemeine Formulierung derart ungenau ist, dass sie das Legalitätsprinzip in Strafsachen missachten würde.

B.24.3. Die angefochtene Bestimmung stellt keine Handlungen unter Strafe und sieht keine Strafen für bestimmte Straftaten vor. Im Gegensatz zum Vorbringen der klagenden Parteien beinhaltet sie auch keine automatische Zuordnung dahingehend/dahin, dass der identifizierte Endnutzer einer Guthabenkarte die Straftaten begangen hat, die nach Auswertung der Nutzung dieser Guthabenkarte entdeckt oder bewiesen werden.

Artikel 127 § 1 Absatz 3 des Gesetzes vom 13. Juni 2005 regelt nur die widerlegbare Vermutung, dass dieser Endnutzer auch derjenige ist, der diese Guthabenkarte benutzt. Das Legalitätsprinzip in Strafsachen findet keine Anwendung auf eine solche Bestimmung.

B.25. Artikel 6 Absatz 2 der Europäischen Menschenrechtskonvention bestimmt:

« Jede Person, die einer Straftat angeklagt ist, gilt bis zum gesetzlichen Beweis ihrer Schuld als unschuldig ».

Artikel 48 Absatz 1 der Charta bestimmt:

« Jede angeklagte Person gilt bis zum rechtsförmlich erbrachten Beweis ihrer Schuld als unschuldig ».

Gemäß diesen Bestimmungen wird bis zum gesetzlichen Nachweis seiner Schuld vermutet, dass der wegen einer strafbaren Handlung Angeklagte unschuldig ist.

Gesetzliche Vermutungen stehen grundsätzlich nicht im Widerspruch der Unschuldsvermutung (in diesem Sinne: EuGHMR, 7. Oktober 1988, *Salabiaku gegen Frankreich*, § 28; 20. März 2001, *Telfner gegen Österreich*, § 16). Sie müssen jedoch einen vernünftigen Zusammenhang der Verhältnismäßigkeit zu dem gesetzmäßig angestrebten Ziel aufweisen (EuGHMR, 23. Juli 2002, *Janosevic gegen Schweden*, § 101; 23. Juli 2002, *Västberga Taxi Aktiebolag und Vulic gegen Schweden*, § 113), wobei der Schweregrad der Sache zu berücksichtigen ist und wobei das Recht der Verteidigung gewahrt werden muss (EuGHMR, 4. Oktober 2007, *Anghel gegen Rumänien*, § 60).

B.26.1. Ursprünglich sah der Vorentwurf, der zum angefochtenen Gesetz geführt hat, vor, dass die identifizierte Person für die Nutzung des elektronischen Kommunikationsdienstes, der ihm bereitgestellt wird, « verantwortlich » ist. In seinem Guthaben Nr. 59.423/4 vom 15. Juni 2016 hat die Gesetzgebungsabteilung des Staatsrats diesbezüglich auf Folgendes hingewiesen:

« À l'article 127, § 1er, alinéa 3, en projet, la section de législation n'aperçoit pas quelle est la portée concrète de la règle en projet, à savoir celle qui prévoit que la personne physique ou morale identifiée est ' responsable ' de l'utilisation du service de communications électroniques qui lui est fourni : quelle est la responsabilité ainsi visée ? S'agit-il de la responsabilité contractuelle à l'égard de l'opérateur, d'une responsabilité aquilienne à l'égard de tiers, ou encore d'une responsabilité pénale ?

Le texte en projet sera revu afin de préciser expressément quelle est la teneur et la portée de la responsabilité envisagée, spécialement si une quelconque responsabilité pénale est ainsi couverte » (*Parl. Dok.*, Kammer, 2015 2016, DOC 54-1964/001, SS. 46-47).

Vor dem Hintergrund dieses Gutachtens hat der Gesetzgeber jeden Verweis auf die « Verantwortung » des Endnutzers aus dem Entwurf entfernt. Während der Vorarbeiten hat er die endgültige Fassung der angefochtenen Bestimmung wie folgt erläutert:

« Le nouvel alinéa introduit a été revu en profondeur suite à l'avis du Conseil d'État qui estimait qu'il n'apercevait pas la portée concrète de la règle en projet.

Le principe selon lequel la personne identifiée est en principe l'utilisateur effectif du service de communications électroniques (sauf preuve contraire) permet d'éviter qu'une personne s'identifie à la place d'un tiers qui utilise effectivement le service de communications électroniques pour cacher l'identité de ce tiers » (ebenda, S. 9).

B.26.2. Die angefochtene Bestimmung begründet folglich keine automatische strafrechtliche Verantwortung oder objektive Haftung des identifizierten Endnutzers einer Guthabenkarte für die Nutzung dieser Karte durch einen Dritten. Sie hat in erster Linie eine Warnfunktion, da sie den Grundsatz jeder strafrechtlichen Untersuchung und jeder Untersuchung durch die Nachrichten- und Sicherheitsdienste in Erinnerung ruft, nämlich den Grundsatz, dass jeder Eigentümer oder jeder gewöhnliche Nutzer eines Gegenstandes vermutlich derjenige ist, der ihn benutzt hat, um eine Straftat zu begehen oder die nationale Sicherheit zu gefährden. Die Ermittlungspersonen nehmen von diesem Grundsatz Abstand, sobald er durch die gesammelten Beweiselemente widerlegt ist.

Außerdem ist die angefochtene Bestimmung, wie in B.16.11.2 ausgeführt wurde, in Verbindung mit den Artikeln 5 und 6 des königlichen Erlasses vom 27. November 2016 zu lesen, die die Möglichkeit zum Überlassen der Guthabenkarte einschränken und den Endnutzer dazu verpflichten, den Betreiber binnen vierundzwanzig Stunden vom Diebstahl oder Verlust der Karte in Kenntnis zu setzen. Diese Bestimmungen tragen in ihrer Gesamtheit zur Sachdienlichkeit von Artikel 127 des Gesetzes vom 13. Juni 2005 bei, da sie die Identifizierbarkeit des tatsächlichen Nutzers einer Guthabenkarte vereinfachen sollen.

B.26.3. Die angefochtene Bestimmung hängt daher mit den Zielen zusammen, die der Gesetzgeber mit Artikel 127 des Gesetzes vom 13. Juni 2005 verfolgt, insbesondere in Notsituationen und bei Untersuchungen, die durch Zeitdruck gekennzeichnet sind.

B.26.4. Die angefochtene Bestimmung spielt außerdem oft eine Rolle im Rahmen von Straftaten oder Bedrohungen für die nationale Sicherheit, die schwerwiegende Folgen für die körperliche Unversehrtheit von Personen haben oder erhebliche Unruhe in der Gesellschaft verursachen können.

B.26.5. Der identifizierte Endnutzer verfügt über verschiedene Möglichkeiten, um sich gegen strafrechtliche Verfolgungen zu verteidigen, die sich aus der Nutzung seiner Guthabenkarte durch einen Dritten ergeben könnten. Wenn er den Ermittlungspersonen mitteilt, wer seine Guthabenkarte benutzt hat, müssen sie die Beteiligung dieser Person untersuchen.

Die angefochtene Bestimmung regelt im Übrigen nur eine widerlegbare Vermutung, die der Angeklagte mit allen rechtlichen Mitteln widerlegen kann. Sie verbietet ihm nicht, alle tatsächlichen Elemente vorzubringen, die seine Beteiligung an den begangenen Straftaten oder an den untersuchten Bedrohungen für die nationale Sicherheit widerlegen.

Ferner lässt die angefochtene Bestimmung den Grundsatz unberührt, dass es in einem Strafprozess der Staatsanwaltschaft obliegt, die Schuld des Angeklagten zu beweisen. Es ist Aufgabe des Strafrichters, den Beweiswert aller Beweiselemente einschließlich der Erläuterungen des Angeklagten zu untersuchen und dabei dessen Recht auf ein faires Verfahren zu beachten.

Da die angefochtene Bestimmung folglich das Verteidigungsrecht des Angeklagten nicht beeinträchtigt, stellt sie auch die Unschuldsvermutung nicht in Frage.

B.26.6. Im Gegensatz zum Vorbringen der klagenden Parteien gilt das Vorstehende ebenso für die Beteiligung des identifizierten Endnutzers an den in den Artikeln 137 bis 141*ter* des Strafgesetzbuches erwähnten terroristischen Straftaten. Er kann dann nur als Mittäter oder Komplize an solchen Straftaten verurteilt werden, wenn die Staatsanwaltschaft alle konstitutiven Elemente dieser Straftaten einschließlich des Absichtselements, was ihn anbelangt, beweist.

Das gutgläubige Bereitstellen einer Guthabenkarte durch einen Endnutzer, der nicht annehmen konnte, dass sie dazu verwendet werden würde, eine solche Straftat zu begehen oder vorzubereiten, kann an sich keine strafrechtliche Verurteilung rechtfertigen.

B.26.7. Vorbehaltlich der in B.26.2 und B.26.6 erwähnten Auslegungen ist der dritte Klagegrund unbegründet.

In Bezug auf den vierten Klagegrund

B.27.1. Im vierten Klagegrund führen die klagenden Parteien an, dass Artikel 3 des angefochtenen Gesetzes gegen die Artikel 10, 11 und 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8 und 52 der

Charta, mit den Artikeln 2 Buchstabe a, 6, 13 und 22 der Richtlinie 95/46/EG und mit den Artikeln 1, 2, 3, 5, 6, 9 und 15 der Richtlinie 2002/58/EG verstoße. Der Klagegrund setzt sich aus fünf Teilen zusammen.

B.27.2. Im ersten Teil führen sie an, dass die angefochtene Bestimmung den Nachrichten- und Sicherheitsdiensten ermögliche, auf die nach Artikel 127 des Gesetzes vom 13. Juni 2005 gesammelten Identifizierungsdaten zuzugreifen, ohne diese Zugriffsmöglichkeit auf schwere Straftaten zu beschränken.

Im zweiten Teil führen sie an, dass diese Zugriffsmöglichkeit der Nachrichten- und Sicherheitsdienste keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen werde.

Im dritten Teil führen sie an, dass die angefochtene Bestimmung die materiellen und prozeduralen Voraussetzungen dieser Zugriffsmöglichkeit unzureichend präzisiere.

Im vierten Teil führen sie an, dass die angefochtene Bestimmung die Nachrichten- und Sicherheitsdienste, die auf die nach Artikel 127 des Gesetzes vom 13. Juni 2005 verarbeiteten Identifizierungsdaten zugreifen könnten, nicht verpflichte, die betroffene Person davon in Kenntnis zu setzen, damit sie ihr Recht auf eine wirksame richterliche Kontrolle wahrnehmen könne.

Im fünften Teil führen sie an, dass die angefochtene Bestimmung nicht ausschließe, dass ausländischen Nachrichten- und Sicherheitsdiensten der Zugriff auf diese Daten ermöglicht werde.

Angesichts ihres gegenseitigen Zusammenhangs sind diese Teile zusammen zu prüfen.

B.28.1. Nach Artikel 1 Absatz 3 der Richtlinie 2002/58/EG gilt diese Richtlinie « nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines

wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich ».

Nach Artikel 2 Absatz 2 Buchtstabe a der Datenschutz-Grundverordnung findet diese Verordnung « keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt ». Nach Artikel 2 Absatz 2 Buchstabe d der Datenschutz-Grundverordnung findet sie auch keine Anwendung auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

In seinem Urteil vom 6. Oktober 2020 in Sachen *La Quadrature du Net u.a.* (C-511/18, C-512/18 und C-520/18), hat die Große Kammer des Gerichtshofs der Europäischen Union entschieden:

« 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 ».

B.28.2. Die angefochtene Bestimmung fügt einen neuen Artikel 16/2 § 2 in das Gesetz vom 30. November 1998 ein. Nach dieser Bestimmung können die Nachrichten- und Sicherheitsdienste im Interesse der Erfüllung ihrer Aufträge die Mitwirkung einer Bank oder eines Finanzinstituts anfordern, um die Identifizierung des Endnutzers einer Guthabenkarte auf der Grundlage der Bezugsnummer eines elektronischen Bankgeschäfts vorzunehmen, das sich auf diese Guthabenkarte bezieht und vorher vom betreffenden Unternehmen mitgeteilt worden ist.

B.28.3. Da die angefochtene Bestimmung nur im Rahmen der Aufträge der Nachrichten- und Sicherheitsdienste Anwendung findet, fällt sie nicht in den Anwendungsbereich des Rechts der Europäischen Union. Folglich ist der Klagegrund unzulässig, sofern damit ein Verstoß gegen die angeführten Bestimmungen der Charta, der Datenschutz-Grundverordnung oder der Richtlinie 2002/58/EG geltend gemacht wird.

B.29.1. Der Zugriff einer Behörde auf Bankdaten fällt in den Anwendungsbereich des Rechts auf Achtung des Privatlebens, unabhängig davon, ob diese Daten als sensibel einzustufen sind oder ob sie mit der Berufsausübung zusammenhängen (EuGHMR, 7. Juli 2005, *M.N. u.a. gegen San Marino*, §§ 51-55; 1. Dezember 2015, *Brito Ferrinho Bexiga Villa Nova gegen Portugal*, § 44; 27. April 2017, *Sommer gegen Deutschland*, § 48).

B.29.2. Der Zugriff einer Behörde auf Bankdaten muss auf einer spezifischen gesetzlichen Grundlage beruhen, die dessen Gegenstand sowie die Schwelle, um sich Zugriff darauf zu verschaffen, klar und unzweideutig eingrenzt. Dieser Gegenstand muss auf dasjenige beschränkt sein, was im Lichte des verfolgten legitimen Ziels notwendig ist, da ein zu weitreichender Zugriff auf Bankdaten dem Staat erlauben würde, ein detailliertes Bild vom Privatleben der betroffenen Person zu gewinnen. Der Staat darf nur dann auf solche Daten zugreifen, wenn er über konkrete Anhaltspunkte verfügt, dass der Inhaber des Bankkontos an einer Straftat beteiligt ist. Ebenso müssen im Gesetz Maßnahmen gegen Missbrauch vorgesehen sein, einschließlich der Garantie, dass die Daten nicht länger aufbewahrt werden, als es im Lichte der geführten Untersuchung notwendig ist. Schließlich muss eine wirksame richterliche Kontrolle hinsichtlich der Einhaltung dieser materiellen und prozeduralen Voraussetzungen bestehen (EuGHMR, 27. April 2017, *Sommer gegen Deutschland*, §§ 57-63).

B.30.1. Die angefochtene Bestimmung präzisiert, welche Dienste über die in B.28.2 erwähnte Ermächtigung verfügen und welche Stellen verpflichtet sind, mitzuwirken.

Sie grenzt auch in zweifacher Hinsicht das Ziel der angefochtenen Maßnahme ein. Erstens soll durch sie entweder der in Artikel 127 des Gesetzes vom 13. Juni 2005 erwähnte Endnutzer einer Guthabenkarte oder die Guthabenkarte, die von einer bestimmten Person benutzt wird, identifiziert werden. Zweitens muss diese Identifizierung mit den Aufträgen der Nachrichten- und Sicherheitsdienste zusammenhängen.

B.30.2. Der Gegenstand der Untersuchungshandlung ist auf ein spezifisches Bankgeschäft beschränkt, nämlich auf dasjenige, über das eine Guthabenkarte gekauft wurde. Eine solche Untersuchungshandlung erlaubt es den Nachrichten- und Sicherheitsdiensten nur, Identifizierungsdaten in Erfahrung zu bringen, verschafft ihnen jedoch an sich weder Verkehrs- oder Standortdaten noch Zugriff auf die geführte Kommunikation.

Die angefochtene Bestimmung erlaubt es ihnen auch nicht, nur mit dieser Untersuchungshandlung andere finanzielle Informationen bezüglich des Inhabers des Bankkontos in Erfahrung zu bringen. Folglich ermöglicht sie es ihnen nicht, sich bloß anhand der gewonnenen Identifizierungsdaten ein Bild vom Ausgabeverhalten oder einem anderen sensiblen Datenelement in Bezug auf den Inhaber des Bankkontos zu machen.

Wie in B.15.3 ausgeführt wurde, können diese Identifizierungsdaten anschließend zwar mit anderen Daten verknüpft werden und kann die angefochtene Bestimmung dementsprechend zur Freigabe solcher sensiblen Informationen beitragen, jedoch müssen diese Informationen dann anhand anderer Untersuchungshandlungen gesammelt werden, bei denen ihrerseits die einschlägigen Rechtsvorschriften und die Grundrechte der betroffenen Person zu beachten sind.

B.30.3. Wie in B.3.3 ausgeführt wurde, kann die Identifizierung aufgrund der angefochtenen Bestimmung in Abhängigkeit von der Identifizierungsmethode, für die sich der Endnutzer beim Erwerb der Guthabenkarte entschieden hat, notwendig sein.

Wenn er sich beim Erwerb der Guthabenkarte für die Identifizierung im Wege eines Online-Zahlungsvorgangs entscheidet, können die Nachrichten- und Sicherheitsdienste ihn nur identifizieren, wenn sie über die Bezugsnummer des elektronischen Bankgeschäfts verfügen und diese sowohl mit der Guthabenkarte als auch der Identität des Endnutzers verknüpfen können (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1964/001, SS. 14-16). Diese Identifizierungsmethode ist in Artikel 17 des königlichen Erlasses vom 27. November 2016 geregelt, der festlegt:

« § 1. Betreffende Unternehmen können den Endnutzer auf der Grundlage eines elektronischen Online-Zahlungsvorgangs identifizieren, der spezifisch für den Kauf oder das Aufladen der Guthabenkarte ausgeführt wird.

Diese Methode unterliegt folgenden Bedingungen:

1. Der Zahlungsvorgang muss von einem in Artikel I.9 Nr. 2 Buchstabe *a), b), c)* und *d)* des Wirtschaftsgesetzbuches erwähnten Zahlungsdienstleister bearbeitet werden.

2. Der Zahlungsdienstleister unterliegt dem Gesetz vom 11. Januar 1993 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung.

3. Binnen achtzehn Monaten nach dem mit der Guthabenkarte verbundenen Zahlungsvorgang muss eine neue Identifizierung erfolgen.

4. Der Endnutzer gibt in einem Online-Formular des betreffenden Unternehmens mindestens seinen Namen, seinen Vornamen, seinen Geburtsort und sein Geburtsdatum ein.

§ 2. Das betreffende Unternehmen speichert die Referenz des Zahlungsvorgangs und die Daten des Online-Formulars auf Vorrat ».

B.30.4. Da die angefochtene Bestimmung die Nachrichten- und Sicherheitsdienste nur ermächtigt, die angefochtene Untersuchungshandlung « im Interesse der Erfüllung ihrer Aufträge » vorzunehmen, müssen sie dabei immer über konkrete Anhaltspunkte verfügen, dass die Identifizierung des Endnutzers einer Guthabenkarte im Rahmen der Aufträge notwendig ist, die in Artikel 7 (Staatssicherheit) und Artikel 11 (Allgemeiner Nachrichten- und Sicherheitsdienst) des Gesetzes vom 30. November 1998 abschließend aufgezählt sind. Da sich alle diese Aufträge auf vitale Interessen der Nation beziehen, liegt beim Ergreifen dieser Maßnahme immer zumindest eine Bedrohung vor, dass ein Ereignis mit sehr schwerwiegenden Folgen für die Gesellschaft eintreten könnte.

B.30.5. Die angefochtene Bestimmung garantiert, dass die Anforderung durch den Dienstleister oder seinen Beauftragten erfolgt und dass sie schriftlich erfolgt oder binnen vierundzwanzig Stunden schriftlich bestätigt wird. Außerdem verlangt Artikel 16/2 § 4 des Gesetzes vom 30. November 1998, dass die Nachrichten- und Sicherheitsdienste ein Register aller angeforderten Identifizierungen führen. Sie müssen diese Liste dem Ständigen Ausschuss N monatlich zukommen lassen.

Die klagenden Parteien führen in diesem Zusammenhang an, dass die angefochtene Bestimmung nicht verlange, dass die Anforderung des Dienstleisters oder seines Beauftragten mit Gründen versehen werde. Eine solche Verpflichtung würde den geheimen Charakter und die Wirksamkeit der von den Nachrichten- und Sicherheitsdiensten geführten Untersuchungen jedoch gefährden.

B.30.6. Die angefochtene Bestimmung garantiert keine spezifische richterliche Kontrolle hinsichtlich der angefochtenen Untersuchungsmaßnahme. Wie in B.14.3 ausgeführt wurde, reichen im Rahmen der Verarbeitung bloßer Identifizierungsdaten und des Zugriffs auf diese allerdings die gemeinrechtlichen Rechtsbehelfe aus (EuGHMR, 30. Januar 2020, *Breyer gegen*

Deutschland, § 106). Die betroffene Person verfügt in diesem Zusammenhang über die in B.16.10 erwähnten Rechtsbehelfe.

B.30.7. Da die angefochtene Untersuchungshandlung eine gewöhnliche Methode zum Sammeln von Daten ist, gelten die in Artikel 43/1 des Gesetzes vom 30. November 1998 erwähnte Kontrolle durch den Verwaltungsausschuss und die in den Artikeln 43/2 bis 43/8 des Gesetzes vom 30. November 1998 erwähnte nachträgliche Kontrolle durch den Ständigen Ausschuss-N insofern nicht.

Angesichts der eingeschränkten Tragweite der angefochtenen Bestimmung, des fundamentalen Interesses der nationalen Sicherheit, des Umstands, dass die Nachrichten- und Sicherheitsdienste mit der angefochtenen Maßnahme nur Identifizierungsdaten in Erfahrung bringen können, und der in B.30.5 erwähnten Garantien reicht dieses Fehlen einer Kontrolle nicht aus, um schlussfolgern zu können, dass die angefochtene Bestimmung das Recht auf Achtung des Privatlebens verletzt.

B.30.8. Die klagenden Parteien führen außerdem an, dass der Gerichtshof den Gesetzgeber in seinen Entscheiden Nr. 145/2011 vom 22. September 2011 und Nr. 41/2019 vom 14. März 2019 dazu verpflichtet habe, eine aktive Pflicht zur Inkenntnissetzung jeder Person durch die Nachrichten- und Sicherheitsdienste vorzusehen, die Gegenstand einer Untersuchung dieser Dienste gewesen sei, sobald die Geheimhaltungspflicht im Rahmen der Untersuchung aufgehoben worden sei.

Der Gerichtshof hat dies allerdings nur für die außergewöhnlichen Methoden zum Sammeln von Daten im Sinne der Artikel 18/12, 18/14 und 18/17 des Gesetzes vom 30. November 1998 gefordert, die es den Nachrichten- und Sicherheitsdiensten erlauben, den Inhalt von Kommunikation in Erfahrung zu bringen. Er erwog dabei, dass diese Methoden am meisten in das Privatleben der betroffenen Person eingreifen. Er hat dies demgegenüber weder für die gewöhnlichen Methoden zum Sammeln von Daten noch für Untersuchungshandlungen gefordert, die sich nur auf das Gewinnen von Identifizierungsdaten beziehen.

B.30.9. Sofern die klagenden Parteien schließlich anführen, dass die angefochtene Bestimmung es erlaube, dass die Nachrichten- und Sicherheitsdienste die gewonnenen Identifizierungsdaten mit ausländischen Nachrichten- und Sicherheitsdiensten teilten, reicht es

aus, festzustellen, dass eine solche Zusammenarbeit nicht Gegenstand der angefochtenen Bestimmung ist, sondern des von ihnen nicht angefochtenen Artikels 20 des Gesetzes vom 30. November 1998.

B.30.10. Vorbehaltlich der in B.30.4 erwähnten Auslegung ist der vierte Klagegrund unbegründet.

Aus diesen Gründen:

Der Gerichtshof

- erklärt Artikel 2 des Gesetzes vom 1. September 2016 « zur Abänderung von Artikel 127 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation und von Artikel 16/2 des Grundlagengesetzes vom 30. November 1998 « über die Nachrichten- und Sicherheitsdienste » für nichtig, wenn auch nur in dem Umfang, in dem er nicht bestimmt, welche Identifizierungsdaten gesammelt und verarbeitet werden und welche Identifizierungsdokumente berücksichtigt werden können;

- erhält die Folgen der für nichtig erklärten Bestimmung bis zum Inkrafttreten einer Gesetzesnorm, in der diese Identifizierungsdaten und -dokumente aufgezählt werden, und längstens bis einschließlich 31. Dezember 2022 aufrecht;

- weist die Klage vorbehaltlich der in B.8.7.3, B.16.6, B.16.8.5, B.16.8.7, B.26.2, B.26.6 und B.30.4 erwähnten Auslegungen im Übrigen zurück.

Erlassen in niederländischer, französischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 18. November 2021.

Der Kanzler, Der Präsident,

P.-Y. Dutilleux L. Lavrysen