WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN
LOIS, DECRETS, ORDONNANCES ET REGLEMENTS

GRONDWETTELIJK HOF

[2021/205605]

Uittreksel uit arrest nr. 158/2021 van 18 november 2021

Rolnummer 6672

In zake : het beroep tot vernietiging van de wet van 1 september 2016 « tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst », ingesteld door Patrick Van Assche en anderen.

Het Grondwettelijk Hof,

samengesteld uit de voorzitters L. Lavrysen en P. Nihoul, de rechters J.-P. Moerman, T. Giet, R. Leysen, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne en D. Pieters, en, overeenkomstig artikel 60*bis* van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, emeritus voorzitter F. Daoût en emeritus rechter T. Merckx-Van Goey, bijgestaan door de griffier P.-Y. Dutilleux, onder voorzitterschap van voorzitter L. Lavrysen,

wijst na beraad het volgende arrest :

I. *Onderwerp van het beroep en rechtspleging*

Bij verzoekschrift dat aan het Hof is toegezonden bij op 7 juni 2017 ter post aangetekende brief en ter griffie is ingekomen op 8 juni 2017, is beroep tot vernietiging ingesteld van de wet van 1 september 2016 « tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst » (bekendgemaakt in het *Belgisch Staatsblad* van 7 december 2016), door Patrick Van Assche, Christel Van Akeleyen en Karina De Hoog, bijgestaan en vertegenwoordigd door Mr. D. Pattyn, advocaat bij de balie van West-Vlaanderen.

(...)

II. *In rechte*

(...)

B.1.1. De wet van 1 september 2016 « tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst » (hierna : de bestreden wet) bepaalt :

« HOOFDSTUK 1. - Voorwerp

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

HOOFDSTUK 2. - Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 2. In artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie, gewijzigd bij de wetten van 4 februari 2010, 10 juli 2012, 27 maart 2014 en 29 mei 2016, worden de volgende wijzigingen aangebracht :

1° in paragraaf 1 worden de volgende wijzigingen aangebracht :

a) in de Franse tekst, in het eerste lid worden de woorden ' aux canaux de vente de services de communications électroniques, aux entreprises fournissant un service d'identification ' ingevoegd tussen de woorden ' visés à l'article 126, § 1er, alinéa 1er, ' en de woorden ' ou aux utilisateurs finals ';

b) in het eerste lid worden de woorden ' de verkoopkanalen van elektronische-communicatiediensten, de ondernemingen die een identificatiedienst verstrekken ' ingevoegd tussen de woorden ' bedoeld in artikel 126, § 1, eerste lid,' en de woorden ' of aan de eindgebruikers ';

c) tussen het eerste en het tweede lid worden zeven leden ingevoegd, luidende :

' Wat de identificatie van de eindgebruiker betreft, is de operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, verantwoordelijk voor de verwerking in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.

Wanneer de eindgebruiker een identificatiedocument voorlegt waarop het rijksregisternummer staat, verzamelt de operator, de aanbieder bedoeld in artikel 126, § 1, eerste lid, het verkoopkanaal van elektronische-communicatiediensten of de onderneming die een identificatiedienst verstrekt, dat nummer.

Het verkoopkanaal van elektronische-communicatiediensten bewaart geen identificatiegegevens of -documenten, die worden overgezonden naar de operator, naar de aanbieder bedoeld in artikel 126, § 1, eerste lid, of naar de onderneming die een identificatiedienst verstrekt.

Indien een rechtstreekse invoer in de computersystemen van de operator, van de aanbieder bedoeld in artikel 126, § 1, eerste lid, of van de onderneming die een identificatiedienst verstrekt, niet mogelijk is, mag het verkoopkanaal van elektronische-communicatiediensten een kopie maken van het identificatiedocument, waaronder van de Belgische elektronische identiteitskaart, maar deze kopie wordt uiterlijk na de activering van de elektronische-communicatiedienst vernietigd.

De operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, bewaart een kopie van de andere identificatiedocumenten dan de Belgische elektronische identiteitskaart.

De verzamelde identificatiegegevens en -documenten worden bewaard overeenkomstig artikel 126, § 3, eerste lid. '

2° paragraaf 3 wordt aangevuld met een lid, luidende :

' De in dit koninklijk besluit gedefinieerde, niet-geïdentificeerde eindgebruikers van voorafbetaalde kaarten die zijn gekocht voor de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 1, identificeren zich binnen de termijn die wordt vastgesteld door de operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, waarbij deze termijn niet langer mag zijn dan zes maanden na de bekendmaking van het koninklijk besluit bedoeld in paragraaf 1. Het in paragraaf 2 bedoelde verbod geldt pas na het einde van de termijn die aan de eindgebruiker wordt toegestaan om zich te identificeren. '

3° in paragraaf 4 worden de volgende wijzigingen aangebracht :

a) in de Franse tekst, worden de woorden ' ou un fournisseur visé à l'article 126, § 1er, alinéa 1er, ' ingevoegd tussen de woorden ' un opérateur ' en de woorden ' ne respecte pas les mesures techniques et administratives qui lui sont imposées ';

b) de woorden ' binnen de door de Koning vastgestelde termijn ' worden opgeheven;

c) de woorden ' of een aanbieder bedoeld in artikel 126, § 1, eerste lid, ' worden ingevoegd tussen de woorden ' een operator ' en de woorden ' niet voldoet aan de hem opgelegde technische en administratieve maatregelen ';

d) in de Franse tekst worden de woorden ' dans le délai fixé ' vervangen door de woorden ' par le présent article ou ';

e) tussen de woorden ' niet voldoen aan de hen ' en de woorden ' opgelegde technische en administratieve maatregelen ' worden de woorden ' door dit artikel of door de Koning ' ingevoegd;

4° in paragraaf 5 worden de volgende wijzigingen aangebracht :

a) in de Franse tekst, in het eerste lid, worden de woorden ' et les fournisseurs visés à l'article 126, § 1er, alinéa 1er,' ingevoegd tussen de woorden ' Les opérateurs ' en de woorden ' déconnectent les utilisateurs finals ';

b) in het eerste lid worden de woorden ' en de aanbieders bedoeld in artikel 126, § 1, eerste lid, ' ingevoegd tussen de woorden ' De operatoren ' en de woorden ' sluiten de eindgebruikers ';

c) in de Franse tekst, in het eerste lid, worden de woorden ' dans le délai fixé ' vervangen door de woorden ' par le présent article ou ';

d) in het eerste lid worden de woorden ' binnen de door de Koning vastgestelde termijn ' opgeheven;

e) in het eerste lid worden de woorden ' door dit artikel of door de Koning ' ingevoegd tussen de woorden ' niet voldoen aan de hen ' en de woorden ' opgelegde technische en administratieve maatregelen ';

f) het tweede lid wordt opgeheven.

HOOFDSTUK 3. - Wijzigingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst

Art. 3. In artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, ingevoegd bij de wet van 5 februari 2016, worden de volgende wijzigingen aangebracht :

1° het huidige eerste tot vierde lid zullen de paragraaf 1 vormen en in de Franse tekst wordt het woord ' chef ' telkens vervangen door het woord ' dirigeant ';

2° er wordt een paragraaf 2 ingevoegd, luidende :

' § 2. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een bank of financiële instelling om over te gaan tot het identificeren van de eindegebruiker van de in artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie bedoelde voorafbetaalde kaart, op basis van de referentie van een elektronische banktransactie die verband houdt met de voorafbetaalde kaart en die voorafgaand meegedeeld is door een operator of verstrekker in toepassing van paragraaf 1.

De vordering gebeurt schriftelijk door het diensthoofd of zijn afgevaardigde. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze gegevens mondeling vorderen. Deze mondelinge vordering wordt binnen de vierentwintig uur bevestigd door een schriftelijke vordering.

Iedere bank en iedere financiële instelling die wordt gevorderd, verstrekt aan het diensthoofd of zijn afgevaardigde onverwijld de gegevens waar om werd verzocht.

De identificatiegegevens die de inlichtingen- en veiligheidsdiensten binnen het uitoefenen van de in deze paragraaf bedoelde methode ontvangen, zijn beperkt tot de identificatiegegevens bedoeld in paragraaf 1. ';

3° het huidige vijfde lid zal de paragraaf 3 vormen;

4° in het huidige zesde lid, waarvan de tekst paragraaf 4 zal vormen, worden de woorden ' de betrokken inlichtingen- en veiligheidsdiensten ' vervangen door de woorden ' de betrokken inlichtingen- en veiligheidsdienst ' en in de Franse tekst worden de woorden ' et de sécurité ' ingevoegd tussen de woorden ' service de renseignement ' en het woord ' concerné ' ».

B.1.2. De bestreden wet maakt deel uit van de antiterreurmaatregelen die zijn genomen in de nasleep van de terroristische aanslagen te Parijs op 13 november 2015 en te Brussel op 22 maart 2016 (*Parl. St.*, Kamer, 2015-2016, DOC 54-1964/001, p. 2). Artikel 2 van de bestreden wet wijzigt artikel 127 van de wet van 13 juni 2005 « betreffende de elektronische communicatie » (hierna : de wet van 13 juni 2005) met het oog op de afschaffing van de anonimiteit van vooraf betaalde belkaarten. Artikel 3 van de bestreden wet wijzigt artikel 16/2 van de wet van 30 november 1998 « houdende regeling van de inlichtingen- en veiligheidsdiensten » (hierna : de wet van 30 november 1998) om de identificatie van de eindgebruiker van een vooraf betaalde belkaart mogelijk te maken op basis van de onlinebanktransactie waarmee zij is aangekocht.

B.2.1. Het bij artikel 2 van de bestreden wet gewijzigde artikel 127 van de wet van 13 juni 2005 bepaalt :

« § 1. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die aan de operatoren, aan de aanbieders bedoeld in artikel 126, § 1, eerste lid, de verkoopkanalen van elektronische-communicatiediensten, de ondernemingen die een identificatiedienst verstrekken of aan de eindgebruikers worden opgelegd om :

1° in het kader van een noodoproep de oproeplijn te kunnen identificeren;

2° de eindgebruiker te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden bepaald door de artikelen 46*bis*, 88*bis* en 90*ter* tot 90*decies* van het Wetboek van strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Wat de identificatie van de eindgebruiker betreft, is de operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, verantwoordelijk voor de verwerking in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.

Wanneer de eindgebruiker een identificatiedocument voorlegt waarop het rijksregisternummer staat, verzamelt de operator, de aanbieder bedoeld in artikel 126, § 1, eerste lid, het verkoopkanaal van elektronische-communicatiediensten of de onderneming die een identificatiedienst verstrekt, dat nummer.

Het verkoopkanaal van elektronische-communicatiediensten bewaart geen identificatiegegevens of -documenten, die worden overgezonden naar de operator, naar de aanbieder bedoeld in artikel 126, § 1, eerste lid, of naar de onderneming die een identificatiedienst verstrekt.

Indien een rechtstreekse invoer in de computersystemen van de operator, van de aanbieder bedoeld in artikel 126, § 1, eerste lid, of van de onderneming die een identificatiedienst verstrekt, niet mogelijk is, mag het verkoopkanaal van elektronische-communicatiediensten een kopie maken van het identificatiedocument, waaronder van de Belgische elektronische identiteitskaart, maar deze kopie wordt uiterlijk na de activering van de elektronische-communicatiedienst vernietigd.

De operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, bewaart een kopie van de andere identificatiedocumenten dan de Belgische elektronische identiteitskaart.

De verzamelde identificatiegegevens en -documenten worden bewaard overeenkomstig artikel 126, § 3, eerste lid.

De Koning bepaalt, na advies van het Instituut, de tarieven voor de vergoeding van de medewerking van de operatoren en de aanbieders bedoeld in artikel 126, § 1, eerste lid, aan de in het eerste lid, 2°, bedoelde verrichtingen alsook de termijn waarbinnen de operatoren of de abonnees moeten voldoen aan de opgelegde maatregelen.

§ 2. De levering of het gebruik van een dienst of van apparatuur die de uitvoering bemoeilijkt of verhindert van de in § 1 bedoelde verrichtingen, zijn verboden, met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen.

§ 3. Totdat de maatregelen, bedoeld in § 1, in werking treden, is het verbod bedoeld in § 2 niet van toepassing op de mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart.

De in dit koninklijk besluit gedefinieerde, niet-geïdentificeerde eindgebruikers van voorafbetaalde kaarten die zijn gekocht voor de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 1, identificeren zich binnen de termijn die wordt vastgesteld door de operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, waarbij deze termijn niet langer mag zijn dan zes maanden na de bekendmaking van het koninklijk besluit bedoeld in paragraaf 1. Het in paragraaf 2 bedoelde verbod geldt pas na het einde van de termijn die aan de eindgebruiker wordt toegestaan om zich te identificeren.

§ 4. Indien een operator of een aanbieder bedoeld in artikel 126, § 1, eerste lid, niet voldoet aan de hem door dit artikel of door de Koning opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.

§ 5. De operatoren en de aanbieders bedoeld in artikel 126, § 1, eerste lid, sluiten de eindgebruikers die niet voldoen aan de hen door dit artikel of door de Koning opgelegde technische en administratieve maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die eindgebruikers worden op geen enkele wijze vergoed voor de afsluiting ».

B.2.2. Artikel 127 van de wet van 13 juni 2005 heeft steeds als uitgangspunt gehad dat alle eindgebruikers van elektronische-communicatienetwerken identificeerbaar moeten zijn. Initieel legde die bepaling slechts verplichtingen op aan de operatoren, de aanbieders en de eindgebruikers van die diensten. Artikel 127, § 1, eerste lid, bevat een algemene machtiging aan de Koning om de technische en administratieve maatregelen te bepalen om die identificeerbaarheid mogelijk te maken.

Die identificeerbaarheid dient een tweevoudig doel. Ten eerste beoogt zij de goede werking van de spoeddiensten te ondersteunen door toe te laten dat de oproeplijn van een noodoproep wordt geïdentificeerd (artikel 127, § 1, eerste lid, 1°). Ten tweede draagt zij bij aan het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privécommunicatie onder de voorwaarden bepaald door de artikelen 46*bis*, 88*bis* en 90*ter* tot 90*decies* van het Wetboek van strafvordering en door de wet van 30 november 1998 (artikel 127, § 1, eerste lid, 2°).

Artikel 127, § 2, van de wet van 13 juni 2005 verbiedt de levering of het gebruik van diensten of apparatuur die de identificeerbaarheid bemoeilijken, met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te waarborgen.

Artikel 127, § 3, van dezelfde wet voorzag initieel in een tijdelijke uitzondering op dat verbod voor de eindgebruikers van vooraf betaalde belkaarten. Die eindgebruikers waren vrijgesteld van de vereiste om identificeerbaar te zijn zolang de Koning de in artikel 127, § 1, bedoelde technische en administratieve maatregelen nog niet had genomen.

B.2.3. Artikel 2 van de bestreden wet heeft artikel 127 van de wet van 13 juni 2005 op verschillende punten gewijzigd. Ten eerste heeft het het toepassingsgebied ervan uitgebreid door sommige van de erin vervatte verplichtingen ook op te leggen aan de verkoopkanalen van elektronische-communicatiediensten en aan de ondernemingen die een identificatiedienst verstrekken.

Ten tweede heeft die bepaling een aantal aspecten van de identificatie van de eindgebruiker wettelijk verankerd. Zo worden de operator en de aanbieder aangeduid als de verwerkers van persoonsgegevens (artikel 127, § 1, tweede lid). Tevens wordt bepaald dat, behoudens tegenbewijs, de geïdentificeerde persoon wordt geacht zelf de elektronische-communicatiedienst te gebruiken (artikel 127, § 1, derde lid), dat de identificatie dient te gebeuren op grond van een identificatiedocument waarop het rijksregisternummer staat (artikel 127, § 1, vierde lid), en dat het verkoopkanaal van elektronische-communicatiediensten geen kopieën van de identificatiegegevens of -documenten die het naar de operator doorstuurt, mag bewaren (artikel 127, § 1, vijfde tot zevende lid).

Ten derde bevat die bepaling enkele specifieke machtigingen aan de Koning, zoals de machtiging verleend aan de Koning in het nieuwe artikel 127, § 1, achtste lid, van de wet van 13 juni 2005 om de vergoeding van de operatoren en aanbieders te bepalen voor de gevallen waarin zij dienen mee te werken aan de identificatie van de eindgebruikers van hun diensten, alsook om de termijn te bepalen waarbinnen de operatoren en de abonnees dienen te voldoen aan de opgelegde maatregelen. Het nieuwe tweede lid van artikel 127, § 3, van de wet van 13 juni 2005 machtigt de Koning om de termijn te bepalen waarbinnen de eindgebruiker van een vooraf betaalde belkaart die is aangekocht vóór de inwerkingtreding van de bestreden wet, zich dient te identificeren. Die termijn mag niet langer zijn dan zes maanden na de bekendmaking van het koninklijk besluit bedoeld in artikel 127, § 1, van dezelfde wet. Krachtens het nieuwe artikel 127, § 3, tweede lid, van de wet van 13 juni 2005 is de anonimiteit van de vooraf betaalde belkaarten pas opgeheven na afloop van die termijn.

B.2.4. De Koning heeft artikel 127 van de wet van 13 juni 2005, althans voor wat betreft de elektronische-communicatiediensten die worden aangeboden op grond van een vooraf betaalde belkaart, ten uitvoer gelegd bij het koninklijk besluit van 27 november 2016 « betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart » (hierna : het koninklijk besluit van 27 november 2016).

Artikel 2, 4°, van dat koninklijk besluit definieert het geldige identificatiedocument als « de Belgische identiteitskaart of een identiteitskaart van een lidstaat van de Europese Unie, een Belgische elektronische kaart voor buitenlanders, het document dat het nummer vermeldt dat bedoeld is in art. 8, § 1, 2°, van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid of in art. 2, tweede lid, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen of een internationaal paspoort of een officieel document dat, tijdelijk, één van de voormelde documenten vervangt dat werd kwijt geraakt of gestolen, op voorwaarde dat het identificatiedocument origineel, leesbaar en geldig is ».

De artikelen 3 tot 6 van het koninklijk besluit van 27 november 2016 leggen verplichtingen op aan de eindgebruikers van vooraf betaalde belkaarten. Zij moeten zichzelf bij de operator identificeren telkens wanneer die dat vraagt. Wanneer zij een nieuwe vooraf betaalde belkaart kopen, delen zij uiterlijk bij de activering ervan hun identiteit mee aan de operator volgens één van de geldige identificatiemethodes. Het is hun in beginsel verboden hun vooraf betaalde kaart aan derden over te dragen, tenzij in de gevallen en onder de voorwaarden bepaald in artikel 5 van het koninklijk besluit. Wanneer zij hun vooraf betaalde kaart verliezen of wanneer deze wordt gestolen, dienen zij de operator daar binnen de 24 uur van op de hoogte te brengen.

De artikelen 7 tot 9 van hetzelfde koninklijk besluit leggen verplichtingen op aan de operatoren. Zij moesten alle eindgebruikers van vooraf betaalde kaarten die waren verkocht vóór de inwerkingtreding, op 17 december 2016, van dat koninklijk besluit identificeren vóór 7 juni 2017. Sinds de inwerkingtreding van dat koninklijk besluit mogen zij geen nieuwe vooraf betaalde kaarten activeren indien de eindgebruiker nog niet is geïdentificeerd. Indien zij door de eindgebruiker worden verwittigd van het verlies of de diefstal van de vooraf betaalde belkaart, dienen zij die onmiddellijk onbruikbaar te maken.

B.2.5. De artikelen 9 tot 12 van hetzelfde koninklijk besluit bepalen hoe de eindgebruiker van een vooraf betaalde belkaart dient te worden geïdentificeerd en hoe zijn identificatiegegevens worden verwerkt. De operator, de leverancier van een identificatiedienst of het verkoopkanaal van elektronische-communicatiediensten verzamelen die gegevens door de Belgische elektronische identiteitskaart via elektronische weg te lezen, die in te scannen of er een kopie of foto van te maken, met inbegrip van de foto op die kaart en het nummer van die kaart. De operator dient vóór de activering van de vooraf betaalde belkaart te controleren of de voorgelegde identiteitskaart is gestolen of het voorwerp uitmaakt van fraude.

De operator bewaart de identificatiemethode die gebruikt is om de eindgebruiker te identificeren zolang diens identificatiegegevens mogen worden bewaard krachtens artikel 126 van de wet van 13 juni 2005. De door de operator te bewaren gegevens worden vastgelegd afhankelijk van de gekozen identificatiemethode, maar omvatten maximaal de naam en voornaam, het geslacht, de nationaliteit, de geboorteplaats en -datum, het adres van de woonplaats, het e-mailadres en het telefoonnummer, het rijksregisternummer, het nummer van het identiteitsstuk, het land van uitgifte van het document wanneer het een buitenlands document betreft en de geldigheidsdatum van het document, de referenties van de betalingstransactie, het verband van de vooraf betaalde kaart met het product waarvoor de eindgebruiker reeds geïdentificeerd is, en de foto van de eindgebruiker, maar die laatste enkel voor andere documenten dan de Belgische elektronische identiteitskaart. Wanneer de foto op de Belgische elektronische identiteitskaart werd verstrekt aan de operator of de leverancier van een identificatiedienst, vernietigen zij die foto uiterlijk vóór de activering van de vooraf betaalde kaart.

Het koninklijk besluit van 27 november 2016 bepaalt tevens de geldige identificatiemethodes, zijnde de identificatie op basis van de identificatiedocumenten in aanwezigheid van de eindgebruiker (artikel 14), de online-identificatie en elektronische ondertekening via de elektronische identiteitskaart bij de betrokken onderneming (artikel 15), de identificatie via de leverancier van een identificatiedienst (artikel 16), de identificatie op grond van de onlinebetalingstransactie (artikel 17), de productuitbreiding of -migratie (artikel 18) en de verificatie via elektronisch communicatiemiddel (artikel 19).

B.2.6. In de parlementaire voorbereiding werd de afschaffing van de anonimiteit voor de vooraf betaalde belkaarten als volgt verantwoord :

« 1) In 2005 heeft de wetgever in artikel 127, § 3, een afwijking opgenomen voor de voorafbetaalde kaarten ten opzichte van het verbod voor een operator om diensten aan te bieden die het moeilijk of onmogelijk maken om de beller te identificeren. Hij heeft in artikel 127, § 1, eveneens bepaald dat een delegatie kan worden gegeven aan de Koning opdat deze laatste de nadere bepalingen voor de identificatie van de gebruikers van voorafbetaalde kaarten zou vastleggen. De bedoeling van de wetgever bestond erin om een einde te maken aan de anonimiteit voor de voorafbetaalde kaarten.

2) De wetgever, die niet rechtstreeks een einde maakte aan de anonimiteit voor de voorafbetaalde kaarten, had tot doel de penetratie van de mobiele telefonie te bevorderen. Dat doel is helemaal verwezenlijkt vandaag.

3) Het schrappen van de anonimiteit voor de voorafbetaalde kaarten is iets wat de gerechtelijke overheden (1999), de inlichtingen- en veiligheidsdiensten en de nooddiensten die ter plaatse hulp bieden reeds lang vragen. Deze laatsten hebben, bij een noodoproep, het recht om automatisch en systematisch de identiteitsgegevens met betrekking tot de persoon die belt te krijgen, zoals die gedefinieerd zijn in artikel 2, 57°, van de WEC, in het belang van de veiligheid van de burger (zie artikel 107 van de WEC).

4) De voorafbetaalde kaarten zijn wijd verspreid in criminele kringen.

5) De identificatie van de gebruiker van een elektronische-communicatiedienst is het eerste obstakel dat Justitie of de inlichtingen- of veiligheidsdiensten moeten overwinnen alvorens, desgevallend, andere maatregelen te treffen. Zonder identificatie verliezen deze andere maatregelen een groot deel van hun nut.

6) Wanneer Justitie of de inlichtingen- of veiligheidsdiensten vandaag niet in staat zijn om de identificatie van de eindgebruiker te krijgen omdat deze gebruiker op anonieme wijze een voorafbetaalde kaart heeft gekocht, worden ze genoopt om een beroep te doen op andere technieken om toch de gezochte persoon te identificeren. Die indirecte andere technieken houden grotere kosten in en zijn indringender voor de persoonlijke levenssfeer dan een eenvoudige identificatie bij de aankoop van een voorafbetaalde kaart. De identificatie van een persoon die heeft ingetekend op een dienst efficiënter maken door de anonimiteit voor de voorafbetaalde kaarten weg te nemen heeft dus tot gevolg dat de kosten voor Justitie en de inlichtingen- en veiligheidsdiensten (alsook het aantal verzoeken gericht aan de operatoren) dalen en dat een onnodige inbreuk op de persoonlijke levenssfeer van de betrokken persoon en de personen die een band hebben met deze laatste, wordt vermeden.

7) Zoals de Raad van State stelt in zijn advies nr. 58.750/4 van 18 januari 2016 moet enerzijds worden opgemerkt dat alleen de kopers van voorafbetaalde kaarten tot op heden anoniem konden blijven, in tegenstelling tot abonnementhouders, en anderzijds dat vanaf de aanneming van de WEC dit stelsel van anonimiteit is opgevat als zijnde bestemd om een tijdelijk karakter te krijgen. In die context heeft de onderzochte bepaling dus tot gevolg, in rechte en in feite, dat er een ongedifferentieerde behandeling wordt hersteld tussen de gebruikers van de betreffende elektronische-communicatiediensten, en aldus een einde wordt gemaakt aan een tijdelijke, gedifferentieerde behandeling, die gunstiger was voor de gebruikers van voorafbetaalde kaarten.

De nieuwe leden 2 tot 8 van artikel 127, § 1, zijn van toepassing op alle elektronische-communicatiediensten. Het nieuwe tweede lid ingevoerd in paragraaf 3 van artikel 127 is echter specifiek voor de mobiele diensten die worden verstrekt op basis van een voorafbetaalde kaart » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1964/001, pp. 4-6).

B.2.7. Uit het voorgaande volgt dat de identificeerbaarheid van alle eindgebruikers van elektronische-communicatienetwerken reeds bij aanvang het uitgangspunt van artikel 127 van de wet van 13 juni 2005 was en dat de anonimiteit van de eindgebruikers van vooraf betaalde belkaarten steeds als een tijdelijke uitzondering is opgevat. Bovendien was het niet zozeer de wetgever, maar de Koning die de anonimiteit heeft afgeschaft door het koninklijk besluit van 27 november 2016 te nemen.

B.3.1. Het bij artikel 3 van de bestreden wet gewijzigde artikel 16/2 van de wet van 30 november 1998 bepaalt :

« § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst om over te gaan tot :

1° het identificeren van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel;

2° het identificeren van de elektronische communicatiediensten en -middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt.

De vordering gebeurt schriftelijk door het diensthoofd of zijn gedelegeerde. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze gegevens mondeling vorderen. Deze mondelinge vordering wordt binnen vierentwintig uur bevestigd door een schriftelijke vordering.

Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die wordt gevorderd, verstrekt aan het diensthoofd of zijn gedelegeerde de gegevens waar om werd verzocht binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op het voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de elektronische communicatie.

Het diensthoofd of zijn gedelegeerde kan, mits naleving van de principes van proportionaliteit en subsidiariteit en mits de registratie van de raadpleging, de bedoelde gegevens ook verkrijgen met behulp van toegang tot de klantenbestanden van de operator of van de dienstenverstrekker. De Koning bepaalt, op voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de elektronische communicatie, de technische voorwaarden waaronder deze toegang mogelijk is.

§ 2. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een bank of financiële instelling om over te gaan tot het identificeren van de eindegebruiker van de in artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie bedoelde voorafbetaalde kaart, op basis van de referentie van een elektronische banktransactie die verband houdt met de voorafbetaalde kaart en die voorafgaand meegedeeld is door een operator of verstrekker in toepassing van paragraaf 1.

De vordering gebeurt schriftelijk door het diensthoofd of zijn afgevaardigde. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze gegevens mondeling vorderen. Deze mondelinge vordering wordt binnen de vierentwintig uur bevestigd door een schriftelijke vordering.

Iedere bank en iedere financiële instelling die wordt gevorderd, verstrekt aan het diensthoofd of zijn afgevaardigde onverwijld de gegevens waar om werd verzocht.

De identificatiegegevens die de inlichtingen- en veiligheidsdiensten binnen het uitoefenen van de in deze paragraaf bedoelde methode ontvangen, zijn beperkt tot de identificatiegegevens bedoeld in paragraaf 1.

§ 3. Eenieder die weigert de aldus gevraagde gegevens mee te delen of de vereiste toegang te verschaffen, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.

§ 4. Beide inlichtingen- en veiligheidsdiensten houden een register bij van alle gevorderde identificaties en van alle via rechtstreekse toegang verkregen identificaties. Het Vast Comité I ontvangt van de betrokken inlichtingen- en veiligheidsdienst maandelijks een lijst van de gevorderde identificaties en van elke toegang ».

B.3.2. De identificatie op grond van de onlinebanktransactie is één van de geldige identificatiemethoden bedoeld in het koninklijk besluit van 27 november 2016. Artikel 17 van dat koninklijk besluit bepaalt :

« § 1. De betrokken onderneming kan de eindgebruiker identificeren op basis van een elektronische betalingstransactie online specifiek om een voorafbetaalde kaart aan te kopen of te herladen.

Deze methode is onderworpen aan de volgende voorwaarden :

1° de betalingstransactie moet worden afgehandeld via een betalingsdienstaanbieder zoals bedoeld in art. I.9. 2°, *a)*, *b)*, *c)*, en *d)* van het Wetboek van Economisch Recht;

2° de betalingsdienstaanbieder is onderworpen aan de Wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme;

3° er moet een nieuwe identificatie worden uitgevoerd binnen de 18 maanden die volgen op de betalingstransactie die is gelinkt aan de voorafbetaalde kaart;

4° op een online formulier van de betrokken onderneming vult de eindgebruiker op zijn minst zijn naam, zijn voornaam en geboortedatum en -plaats in.

§ 2. De betrokken onderneming slaat de referentie van de betalingstransactie en de gegevens van het online formulier op ».

B.3.3. In de parlementaire voorbereiding werd die verplichte medewerking van banken of financiële instellingen als volgt verantwoord :

« Het koninklijk besluit betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart, zal de manieren bepalen waarop een operator zijn eindgebruikers kan identificeren. Dit kan o.a. gebeuren door verificatie op basis van een online banktransactie.

Laatstgenoemde identificatiemethode vormt de grondslag van voorliggend voorstel. De identificatie via banktransactie houdt in dat de eindgebruiker van een voorafbetaalde kaart (prepaid) zichzelf kan identificeren op basis van een elektronische banktransactie die verband houdt met de voorafbetaalde kaart. Deze methode is onderworpen aan meerdere voorwaarden : (1) de transactie is verbonden aan een bankrekening waarvan de identiteit van de houder vooraf is geverifieerd. Deze methode mag niet worden toegepast in geval van een niet traceerbare bankkaart, (2) de bank is in België gevestigd. De betrokken operator slaat de referentie van de banktransactie op.

Het identificeren van de eindgebruiker van een voorafbetaalde kaart geschiedt via de uitoefening van twee vorderingen :

1° een vordering van een operator van een elektronisch communicatienetwerk, voor het bekomen van een identificatiegegeven (in toepassing van het huidige artikel 16/2) waarop de operator als antwoord de referentie van een banktransactie geeft, en

2° een vordering van een bank of financiële instelling voor het bekomen van de identiteit van de persoon die schuilgaat achter deze banktransactie (in toepassing van de nieuwe § 2 van artikel 16/2).

Op grond van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten hebben de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid bij de Krijgsmacht de bevoegdheid om een operator van een elektronisch communicatienetwerk of een verstrekker van een elektronische communicatiedienst te vorderen om de abonnee of gewoonlijke gebruiker van een elektronische communicatiedienst of -middel te identificeren.

Deze bevoegdheid - die oorspronkelijk ondergebracht werd in de categorie van ' specifieke methoden ' - werd bij wet van 5 februari 2016 tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie (de zogenaamde Potpourriwet 2), geherkwalificeerd als een gewone inlichtingenmethode. In tegenstelling tot de andere gewone methoden werden wel een aantal bijkomende materiële en formele voorwaarden gesteld (bevoegdheid enkel in hoofde van het diensthoofd of zijn gedelegeerde, en niet in hoofde van eender welke inlichtingenagent, verplichte registratie) alsook een bijkomend extern toezichtmechanisme (verplichte maandelijkse notificatie aan het Vast Comité I die op zijn beurt hierover rapporteert aan het Parlement en de bevoegde ministers).

Het opvragen bij een bank of financiële instelling van informatie over banktransacties door een inlichtingen en veiligheidsdienst (artikel 18/15 wet van 30 november 1998) kan daarentegen enkel via de in de wet van 30 november 1998 vastgelegde procedure van toepassing bij de categorie van ' uitzonderlijke methoden '. Deze procedure vereist een voorafgaand eensluidend advies van de BIM-Commissie (de commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten) en de machtiging van het diensthoofd. Uitzonderlijke methoden zijn eveneens onderhevig aan strenge toepassingsvoorwaarden.

De verschillende procedures waar beide vorderingen aan onderhevig zijn zorgt ervoor dat de identificatiemethode via banktransactie - in wezen een identificatie van de gebruiker van een elektronische communicatiedienst - in de feiten een uitzonderlijke methode verwordt. Dit is in strijd met de doelstelling nagestreefd in de Potpourriwet 2.

Daarenboven dient indachtig gehouden te worden dat bij identificeren van de eindgebruiker van een voorafbetaalde kaart de informatie die aan de bank gevraagd wordt enkel dient om de identiteit te achterhalen van degene die een banktransactie verricht heeft, en er bijgevolg niet op gericht is een zicht te krijgen op de financiële situatie van deze persoon. Om informatie omtrent bankrekeningen te verkrijgen blijft de huidige regeling (uitzonderlijke methode) dus van toepassing. Via de gewone methode kan men met andere woorden enkel naam, voornaam, geslacht, nationaliteit, geboorteplaats en -datum, adres en rijksregisternummer van de persoon die gekoppeld is aan het bankrekeningnummer opvragen en dit enkel in het kader van het identificeren van de gebruiker van een prepaid sim kaart.

Er kan tenslotte op gewezen worden dat in het voorliggend voorstel het identificeren van de eindgebruiker van een voorafbetaalde kaart weliswaar een gewone methode wordt, maar dat er toch extra waarborgen gelden ten opzichte van andere gewone methoden. Zo mag de informatie niet door eender wie opgevraagd worden maar is enkel het diensthoofd of zijn gedelegeerde hiertoe gemachtigd. Ook moeten de inlichtingen- en veiligheidsdiensten een register bijhouden van alle gevorderde identificaties en moeten ze maandelijks een lijst van deze vorderingen overmaken aan het Comité I » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1964/001, pp. 14-16).

Ten aanzien van het eerste middel

B.4. In het eerste middel voeren de verzoekende partijen aan dat artikel 2 van de bestreden wet de artikelen 10, 11 en 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8 en 52 van het Handvest van de grondrechten van de Europese Unie (hierna : het Handvest) en met de artikelen 2, *a)*, en 6 van de richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens », schendt, doordat die bepaling een te ruime en een onvoldoende nauwkeurig omschreven machtiging aan de Koning zou verlenen om de inhoud van de bestreden identificatie-verplichting te bepalen.

B.5.1. Het beginsel van gelijkheid en niet-discriminatie sluit niet uit dat een verschil in behandeling tussen categorieën van personen wordt ingesteld, voor zover dat verschil op een objectief criterium berust en het redelijk verantwoord is.

Het bestaan van een dergelijke verantwoording moet worden beoordeeld rekening houdend met het doel en de gevolgen van de betwiste maatregel en met de aard van de ter zake geldende beginselen; het beginsel van gelijkheid en niet-discriminatie is geschonden wanneer vaststaat dat er geen redelijk verband van evenredigheid bestaat tussen de aangewende middelen en het beoogde doel.

B.5.2. Artikel 22 van de Grondwet bepaalt :

« Ieder heeft recht op eerbiediging van zijn privé-leven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.

De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht ».

Artikel 8 van het Europees Verdrag voor de rechten van de mens bepaalt :

« 1. Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn gezinsleven, zijn huis en zijn briefwisseling.

2. Geen inmenging van enig openbaar gezag is toegestaan met betrekking tot de uitoefening van dit recht dan voor zover bij de wet is voorzien en in een democratische samenleving nodig is in het belang van 's lands veiligheid, de openbare veiligheid, of het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, of voor de bescherming van de rechten en vrijheden van anderen ».

Artikel 7 van het Handvest bepaalt :

« Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie ».

Artikel 8 van het Handvest bepaalt :

« 1. Eenieder heeft recht op bescherming van zijn persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.

3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd ».

Artikel 52, lid 1, van het Handvest bepaalt :

« Beperkingen op de uitoefening van de in dit Handvest erkende rechten en vrijheden moeten bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. Met inachtneming van het evenredigheids-beginsel kunnen slechts beperkingen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen ».

Artikel 52, lid 3, van het Handvest bepaalt :

« Voor zover dit Handvest rechten bevat die corresponderen met rechten welke zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend. Deze bepaling verhindert niet dat het recht van de Unie een ruimere bescherming biedt ».

B.5.3. De Grondwetgever heeft gestreefd naar een zo groot mogelijke concordantie tussen artikel 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de rechten van de mens (*Parl. St.*, Kamer, 1992-1993, nr. 997/5, p. 2).

De draagwijdte van dat artikel 8 is analoog aan die van de voormelde grondwetsbepaling, zodat de waarborgen die beide bepalingen bieden, een onlosmakelijk geheel vormen.

Wanneer het Handvest rechten bevat die corresponderen met rechten die zijn gewaarborgd door het Europees Verdrag voor de rechten van de mens, « zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend ». Die bepaling stemt de inhoud en reikwijdte van de door het Handvest gewaarborgde rechten af op de corresponderende rechten die worden gewaarborgd door het Europees Verdrag voor de rechten van de mens.

In de toelichtingen bij het Handvest (2007/C 303/02), bekendgemaakt in het *Publicatieblad* van 14 december 2007, wordt aangegeven dat, onder de artikelen « met dezelfde inhoud en reikwijdte als de daarmee corresponderende artikelen van het EVRM », artikel 7 van het Handvest correspondeert met artikel 8 van het Europees Verdrag voor de rechten van de mens.

Het Hof van Justitie van de Europese Unie herinnert in dat verband eraan dat « artikel 7 van het Handvest, inzake de eerbiediging van het privéleven en van het familie- en gezinsleven, rechten bevat die corresponderen met de [...] rechten [die worden gegarandeerd door artikel 8, lid 1, van het Europees Verdrag voor de rechten van de mens, ondertekend te Rome op 4 november 1950 (hierna : het EVRM),] en dat, overeenkomstig artikel 52, lid 3, van het Handvest, aan dat artikel 7 dus dezelfde inhoud en reikwijdte moeten worden toegekend als die welke aan artikel 8, lid 1, van het EVRM worden toegekend, zoals uitgelegd in de rechtspraak van het Europees Hof voor de Rechten van de Mens » (HvJ, 17 december 2015, C-419/14, *WebMindLicenses Kft.*, punt 70; 14 februari 2019, C-345/17, *Buivids*, punt 65).

Wat artikel 8 van het Handvest betreft, oordeelt het Hof van Justitie dat « zoals in artikel 52, lid 3, tweede zin, daarvan uitdrukkelijk wordt bepaald, [artikel 52, lid 3, eerste zin, van het Handvest] niet [verhindert] dat het Unierecht een ruimere bescherming biedt dan het EVRM », en dat « artikel 8 van het Handvest betrekking heeft op een ander grondrecht dan het in artikel 7 van het Handvest geformuleerde grondrecht, dat geen equivalent heeft in het EVRM » (HvJ, grote kamer, 21 december 2016, C-203/15 en C-698/15, *Tele2 Sverige*, punt 129).

Uit het voorgaande volgt dat, binnen de werkingssfeer van het Europees Unierecht, artikel 22 van de Grondwet, artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 7 van het Handvest analoge grondrechten waarborgen, terwijl artikel 8 van dat Handvest een specifieke rechtsbescherming van persoonsgegevens beoogt.

B.5.4. Krachtens artikel 94, lid 1, van de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) » (hierna : AVG) is de richtlijn 95/46/EG ingetrokken met ingang van 25 mei 2018.

Artikel 5 van de AVG, dat *mutatis mutandis* de inhoud van artikel 6 van de richtlijn 95/46/EG heeft overgenomen, bepaalt :

« 1. Persoonsgegevens moeten :

a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (' rechtmatigheid, behoorlijkheid en transparantie ');

b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (' doelbinding ');

c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (' minimale gegevensverwerking ');

d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (' juistheid ');

e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen (' opslagbeperking ');

f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (' integriteit en vertrouwelijkheid ').

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen (' verantwoordingsplicht ') ».

B.6. Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering.

Een delegatie aan de uitvoerende macht is evenwel niet in strijd met het wettigheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgesteld.

B.7.1. Volgens de Ministerraad is het middel onontvankelijk, aangezien de bestreden bepaling slechts één nieuwe delegatie aan de Koning bevat, meer bepaald de delegatie die werd ingevoegd in het nieuwe artikel 127, § 3, tweede lid, van de wet van 13 juni 2005, en die door de verzoekende partijen niet wordt bestreden. De overige delegaties aan de Koning waren reeds vóór de inwerkingtreding van de bestreden bepaling vervat in artikel 127 van die wet.

B.7.2. Een beroep dat gericht is tegen een verschil in behandeling dat niet uit de bestreden wet voortvloeit, maar reeds is vervat in een vroegere wet, is niet ontvankelijk.

Wanneer de wetgever in een nieuwe wetgeving echter een oude bepaling overneemt en zich op die wijze de inhoud ervan toe-eigent, kan tegen de overgenomen bepaling een beroep worden ingesteld binnen zes maanden na de bekendmaking ervan.

B.7.3. De bestreden bepaling heeft artikel 127 van de wet van 13 juni 2005 op verschillende punten gewijzigd, al bleef de wetgever daarbij, zoals in B.2.7 werd uiteengezet, trouw aan het initiële uitgangspunt van de identificeerbaarheid van alle eindgebruikers van elektronische-communicatienetwerken. Aldus heeft hij zich bij het uitvaardigen van de bestreden bepaling de inhoud van artikel 127 van de wet van 13 juni 2005 toegeëigend.

De exceptie wordt verworpen.

B.8.1. De Commissie voor de bescherming van de persoonlijke levenssfeer (thans de Gegevensbeschermingsautoriteit) heeft in een advies bij het voorontwerp dat tot de bestreden wet heeft geleid enkele opmerkingen geformuleerd met betrekking tot de inachtneming van het wettigheidsbeginsel inzake beperkingen van het recht op eerbiediging van het privéleven :

« 10. Het voorontwerp van wet regelt specifiek deze kwestie, waardoor aan bovenvermelde vormvereiste van een wettelijke basis formeel is voldaan. De Commissie merkt evenwel op dat de wetgever heeft nagelaten enkele essentiële elementen in de wettekst mee op te nemen. Het voorontwerp en de toelichting verwijzen beiden naar de te nemen uitvoeringsmaatrelen inzake de specificaties van de geplande gegevensverwerking, die via Koninklijk Besluit zullen worden vastgelegd, nl. aanduiding van de verantwoordelijke voor de verwerking, bepaling wie toegang heeft tot de gegevens, vastlegging van de bewaartermijn,.... Bij gebrek aan concrete teksten is de Commissie op heden niet in staat een oordeel te vellen over de geplande uitvoeringsmaatregelen. De Commissie wijst er op dat de navolgende uitvoeringsbesluiten (ter uitvoering van artikel 127 van de Telecomwet) haar voorafgaandelijk ter advies moeten worden voorgelegd, eens die beschikbaar zijn, opdat deze kunnen worden getoetst aan de vereisten in het licht van de Privacywet, onder meer de noodzakelijk vereiste van proportionaliteit. Het strekt tot aanbeveling dergelijke adviesvraag voor de uitvoeringsbesluiten mee op te nemen in de eigenlijke wettekst.

[...]

14. Zoals hoger vermeld [...], beveelt de Commissie aan om in de wettekst op te nemen dat de identificatie van de voorafbetaalde kaarten die verkocht werden voor 1 mei 2016 eveneens zal geschieden aan de hand van de identificatiegegevens die krachtens artikel 126 moeten worden bewaard. Het zou niet logisch zijn voor bestaande gebruikers in andere gegevenscategorieën te voorzien. De aard van de gegevens dient wettelijk te worden bepaald. Het uitvoeringsbesluit slaat enkel op de uitvoeringsmaatregelen en de implementatiedatum.

15. De toelichting bij het voorontwerp verduidelijkt bovendien het voornemen om de identificatiegegevens die krachtens artikel 126 moeten worden bewaard aan te vullen met het Rijksregisternummer. Het is wezenlijk deze aanvulling als dusdanig in de eigenlijke wettekst mee op te nemen.

[...]

OM DEZE REDENEN,

de Commissie,

Verleent een gunstig advies onder strikte voorwaarde van de gemaakte opmerkingen en meer in het bijzonder met betrekking tot :

- De vraag om de geplande uitvoeringsbesluiten ter advies aan de Commissie voor te leggen, teneinde o.m. de proportionaliteit te toetsen (randnrs. 10 en 20);

- De expliciete vermelding in de wet betreffende de elektronische communicatie van gebruik van het Rijksregisternummer voor wat uitsluitend prepaidkaarten betreft (randnr. 17);

- Het voorontwerp van wet aan te vullen met de aard van de gegevens, zijnde de identificatiegegevens die moeten worden bewaard krachtens artikel 126, aangevuld met het Rijksregisternummer, en dit zowel voor de kaarten gekocht op 1 mei 2016 of na deze datum, alsook voor de kaarten verkocht voor deze datum (randnrs. 14-15) » (CBPL, advies nr. 54/2015, 15 december 2015, *Parl. St.*, Kamer, 2015-2016, DOC 54-1964/001, pp. 30-34).

Ook de Raad van State, afdeling wetgeving, heeft in een advies bij dat voorontwerp enkele opmerkingen geformuleerd over de inachtneming van het wettigheidsbeginsel inzake beperkingen van het recht op eerbiediging van het privéleven :

« 1.2.4. De machtigingen die bij het ontworpen artikel 127, § 1, zesde en zevende lid, aan de Koning worden verleend, zijn veel te ruim : de wetgever dient vast te stellen in welke gevallen de operator een kopie mag of moet maken van het document waaruit de identiteit van de eindgebruiker kan worden opgemaakt, en hij behoort te bepalen om welk document het gaat.

Voorts moet de wetgever vaststellen welke criteria de Koning moet hanteren om onderscheiden identificatiemethodes vast te leggen met onderscheiden datums van inwerkingtreding, naargelang de vooraf betaalde kaarten vóór of na een door de Koning vastgestelde datum worden geactiveerd. In dat opzicht zou de uitleg in de bespreking van het artikel in hoofdlijnen moeten worden opgenomen in het ontworpen dispositief zelf in de vorm van door de Koning te hanteren criteria en zou die uitleg daarenboven aangevuld moeten worden in de bespreking van het artikel.

1.2.5. Indien het de bedoeling van de steller van het voorontwerp is om de verplichting op te leggen om niet alleen de identificatiegegevens te bewaren - per definitie gedurende de termijn bepaald in artikel 126 van de wet van 13 juni 2005 - maar ook de documenten waaruit die gegevens kunnen worden verkregen, dient de wetgever zelf die verplichting op te leggen en de termijn ervan vast te stellen - die uiteraard niet langer mag zijn dan de termijn bepaald in artikel 126 » (Raad van State, afdeling wetgeving, advies nr. 59.423/4, 15 juni 2016, *Parl. St.*, Kamer, 2015-2016, DOC 54-1964/001, pp. 47-48).

B.8.2. De wetgever heeft die adviezen slechts gedeeltelijk gevolgd. Hij heeft er met name voor gekozen om, in weerwil van die adviezen, niet in de bestreden bepaling op te nemen welke identificatiegegevens mogen worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen. Die keuze werd in de parlementaire voorbereiding als volgt verantwoord :

« Ten eerste is het met uitzondering van het gebruik van het rijksregisternummer, het koninklijk besluit ter uitvoering van artikel 127, § 1, eerste lid, van de wet (het ontwerp van koninklijk besluit ' voorafbetaalde kaarten ') en niet dit artikel dat de te verzamelen identificatiegegevens definieert.

Met uitzondering van het rijksregisternummer zijn de precieze te verzamelen identificatiegegevens immers niet de essentiële elementen van deze kwestie. Overigens vraagt de Commissie voor de bescherming van de persoonlijke levenssfeer in haar eerste advies over het wetsontwerp (advies nr. 54/2015 van 16 december 2015) niet dat de lijst van de te verzamelen gegevens wordt opgenomen in de wet, maar dat alleen de aard van de gegevens wordt vermeld, namelijk de identificatiegegevens die moeten worden bewaard krachtens artikel 126. Om te voldoen aan de vraag van de Privacycommissie bepaalt het wetsontwerp dat de verzamelde identificatiegegevens worden bewaard overeenkomstig artikel 126, § 3, eerste lid, van de wet.

Bovendien worden voor de bewaring van de gegevens, de te bewaren gegevens vastgesteld in het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie en niet in artikel 126. Naar analogie is het het ontwerp van koninklijk besluit ' voorafbetaalde kaarten ' dat de te verzamelen identificatiegegevens omvat en niet artikel 127 van de wet, dat de wettelijke grondslag is van dit koninklijk besluit. Zowel artikel 127 als artikel 126 vormen een beperking op de fundamentele vrijheden.

Uiteindelijk is het niet passend dat de exacte lijst van de te verzamelen identificatiegegevens wordt opgenomen in de wet, gelet op de technische aard van deze gegevens, het feit dat deze gegevens nauw verbonden zijn met de identificatiemethodes die worden ontwikkeld in het koninklijk besluit ' voorafbetaalde kaarten ' in ontwerp (en enkel begrijpelijk zijn als men dat koninklijk besluit leest) en de eventuele noodzaak om ze in de toekomst aan te passen op grond van de lering getrokken uit de praktijk of toekomstige ontwikkelingen.

Ten tweede is het het ontwerp van koninklijk besluit ' voorafbetaalde kaarten ' en niet artikel 127 van de wet dat de volledige lijst zal bepalen van de identificatiedocumenten die worden aanvaard.

Het gaat immers niet om een essentieel onderdeel van de wetgeving (het essentiële onderdeel is daarentegen het feit dat de identificatie moet gebeuren op basis van een geldig identificatiedocument).

Door overigens deze lijst op te nemen zou de wet worden verzwaard (gelet op de talrijke identificatiedocumenten die zouden moeten worden toegestaan) en dit zou als nadeel hebben dat de wet niet makkelijk kan worden aangepast aan de lering die uit de praktijk en ontwikkelingen wordt getrokken.

Ten derde ontwikkelt het wetsontwerp geen criteria om de delegatie aan de Koning te omkaderen met betrekking tot de differentiatie tussen de nieuwe en de oude voorafbetaalde kaarten, zoals gevraagd door de Raad van State. De identificatiemethodes voor de oude en de nieuwe voorafbetaalde kaarten zijn in werkelijkheid immers dezelfde : een eindgebruiker van een nieuwe voorafbetaalde kaart en een eindgebruiker van een oude voorafbetaalde kaart die nog niet geïdentificeerd is, moeten zich volgens dezelfde identificatiemethodes identificeren.

Het wetsontwerp stelt daarentegen rechtstreeks de toepasselijke regels vast (zie het nieuwe lid ingevoegd in paragraaf 3 van artikel 127). De delegatie aan de Koning zal enkel nog slaan op de definitie van wat een reeds geïdentificeerde eindgebruiker van een oude kaart is.

In haar brief van 1 juli 2016 aan de vice-eersteminister en minister voor Telecommunicatie, [...] heeft de Commissie voor de bescherming van de persoonlijke levenssfeer aangegeven dat ze geen enkele opmerking heeft over dit ontwerp » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1964/001, pp. 6-7).

B.8.3.1. Artikel 127 van de wet van 13 juni 2005 regelt zelf het principe van de identificeerbaarheid van de eindgebruiker van zowel oude als nieuwe vooraf betaalde kaarten. Het koppelt de afschaffing van de anonimiteit van vooraf betaalde kaarten aan de datum waarop het uitvoeringsbesluit in werking treedt en voegt daaraan toe dat het vanaf die datum verboden is om diensten of apparatuur te leveren die de identificatie kunnen hinderen. Het bepaalt ook dat de geïdentificeerde eindgebruiker behoudens tegenbewijs zelf wordt geacht de elektronische-communicatiedienst te gebruiken.

Het vermeldt tevens de categorieën van personen aan wie in dit verband verplichtingen worden opgelegd, namelijk de operatoren, de aanbieders, de verkoopkanalen, de ondernemingen die een identificatiedienst aanbieden en de eindgebruikers. Het bepaalt tot slot ook het doel van de identificeerbaarheid, namelijk de goede werking van de nooddiensten, het strafrechtelijk onderzoek en de werking van de inlichtingen- en veiligheidsdiensten.

B.8.3.2. Op het vlak van de identificeerbaarheid verleent artikel 127 van de wet van 13 juni 2005 verschillende machtigingen aan de Koning. Allereerst machtigt het Hem op algemene wijze om de technische en administratieve maatregelen te nemen die in dit verband aan de betrokken partijen moeten worden opgelegd. Tevens dient Hij te bepalen wie de niet-geïdentificeerde eindgebruikers van vooraf betaalde kaarten gekocht vóór de inwerkingtreding van het uitvoeringsbesluit zijn. Hij dient ook de maximale termijn te bepalen waarbinnen de niet-geïdentificeerde eindgebruikers zich bij hun operator moeten identificeren, al begrenst artikel 127 van de wet van 13 juni 2005 die machtiging door te bepalen dat die termijn niet meer dan zes maanden mag bedragen. Tot slot dient de Koning de tarieven te bepalen voor de medewerking van de operatoren en de aanbieders aan de identificatie van een eindgebruiker.

Die machtigingen hebben betrekking op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgesteld.

B.8.4.1. Wat de betrokken identificatiegegevens en identificatiedocumenten betreft, bepaalt artikel 127 van de bestreden wet dat het moet gaan om documenten die het rijksregisternummer bevatten, alsook dat het rijksregisternummer een persoonsgegeven is dat in dit verband dient te worden verzameld en verwerkt. De overige identificatiegegevens, alsook de identificatiedocumenten die in aanmerking komen, worden, in weerwil van de in B.8.1 vermelde adviezen, niet in die wetsbepaling opgesomd.

B.8.4.2. Bovendien heeft de wetgever de Koning geen uitdrukkelijke machtiging gegeven om die identificatiegegevens en identificatiedocumenten nader te bepalen. Dergelijke essentiële elementen van een verwerking van persoonsgegevens kunnen nochtans niet worden begrepen onder de vage machtiging in artikel 127, § 1, eerste lid, van de wet van 13 juni 2005 om de nodige « technische en administratieve maatregelen » te nemen met het oog op de identificeerbaarheid van de eindgebruiker.

De Koning diende die identificatiegegevens en -documenten bijgevolg vast te stellen op grond van de bevoegdheid die Hij aan artikel 108 van de Grondwet ontleent om de verordeningen en de besluiten te nemen die voor de uitvoering van de wetten nodig zijn.

Die algemene uitvoeringsbevoegdheid van de Koning kan te dezen evenwel niet volstaan. Een delegatie van essentiële elementen van een door de Grondwetgever aan de formele wetgever voorbehouden aangelegenheid is immers slechts mogelijk indien de inachtneming van de parlementaire procedure de wetgever niet in staat zou stellen een doelstelling van algemeen belang te verwezenlijken, en op voorwaarde dat hij het onderwerp van die machtiging uitdrukkelijk en ondubbelzinnig vaststelt en dat de door de Koning genomen maatregelen door de wetgevende macht worden onderzocht met het oog op hun bekrachtiging binnen een relatief korte termijn, vastgesteld in de machtigingswet.

B.8.4.3. In de parlementaire voorbereiding verantwoordt de wetgever die manier van werken door te verwijzen naar de technische aard van de identificatiegegevens en identificatiedocumenten, de noodzaak om de oplijsting daarvan te kunnen aanpassen in het licht van gewijzigde inzichten, en het feit dat ook in het kader van de dataretentie die gegevens niet in het bij het arrest van het Hof nr. 57/2021 van 22 april 2021 vernietigde artikel 126 van de wet van 13 juni 2005 zelf werden opgesomd.

Nog afgezien van het feit dat die argumenten de afwezigheid van een uitdrukkelijke en ondubbelzinnige machtiging niet kunnen verklaren, volstaan de technische aard van identificatiegegevens en identificatiedocumenten en de aanpasbaarheid van een dergelijke oplijsting niet om te besluiten dat een verankering ervan in een wetskrachtige norm de wetgever niet in staat zou stellen een doelstelling van algemeen belang te verwezenlijken. Ook een wetskrachtige norm kan immers worden gewijzigd. De Ministerraad toont niet aan dat een wijziging van die identificatiegegevens zo dringend kan zijn dat het normale verloop van de wetgevende procedure niet kan worden gevolgd. Een oplijsting van identificatiegegevens en identificatiedocumenten is ook niet dermate complex dat zij niet in een wetskrachtige norm kan worden opgenomen. Tot slot kan de wetgever een schending van de Grondwet niet rechtvaardigen door te verwijzen naar een andere wetsbepaling die mogelijk dezelfde ongrondwettigheid bevatte.

B.8.4.4. Artikel 127 van de wet van 13 juni 2005 bakent de uitvoeringsbevoegdheid van de Koning om te bepalen welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen, overigens onvoldoende af. Wat de identificatiedocumenten betreft, vermeldt het slechts dat het moet gaan om documenten waarop het rijksregisternummer voorkomt. Wat de andere identificatiegegevens dan het rijksregisternummer betreft, bevat het geen enkele precisering.

B.8.5. Wat het verzamelen en verwerken van de identificatiegegevens en -documenten betreft, bepaalt artikel 127 van de wet van 13 juni 2005 wie de gegevens verzamelt, namelijk het verkoopkanaal of de onderneming die een identificatiedienst aanbiedt. Het bepaalt ook dat het verkoopkanaal die gegevens en documenten niet mag bijhouden en dat het hen dient te vernietigen uiterlijk op het ogenblik van de activering van de vooraf betaalde belkaart.

Wat de wijze van gegevensverwerking betreft, bepaalt artikel 127 van de wet van 13 juni 2005 wie de bevoegde gegevensverwerker is, namelijk de operator of de aanbieder. Het bepaalt tevens dat het verkoopkanaal de verzamelde gegevens overzendt naar de operator, de aanbieder of de onderneming die een identificatiedienst aanbiedt, met rechtstreekse invoer in een computersysteem of middels een kopie van het identificatiedocument. Het bepaalt ook dat de operator en de aanbieder een kopie van elk ander identificatiedocument dan de Belgische elektronische identiteitskaart moeten bewaren en dat de verwerkte identificatiegegevens dienen te worden bewaard krachtens artikel 126, § 3, van de wet van 13 juni 2005.

B.8.6. Wat de sancties betreft, bepaalt artikel 127, §§ 4 en 5, van de wet van 13 juni 2005 dat de operatoren of aanbieders die niet voldoen aan de door de Koning opgelegde technische en administratieve maatregelen, de dienst waarvoor die maatregelen niet zijn genomen, niet meer mogen aanbieden. Tevens bepaalt het dat de eindgebruikers die niet aan de op hen rustende verplichtingen voldoen, zonder vergoeding van het elektronische-communicatienetwerk dienen te worden afgesloten.

B.8.7.1. De verzoekende partijen verwijten de bestreden bepaling voorts dat zij geen aparte criteria bepaalt voor de eindgebruikers van oude en nieuwe vooraf betaalde kaarten.

Artikel 127 van de wet van 13 juni 2005, zoals gewijzigd bij artikel 2 van de bestreden wet, onderwerpt evenwel beide categorieën van eindgebruikers op gelijke wijze aan de vereiste van identificeerbaarheid. Artikel 127, § 3, tweede lid, van die wet bepaalt in dat verband een maximale termijn waarbinnen de eindgebruikers van oude vooraf betaalde kaarten aan de door de Koning bepaalde administratieve en technische maatregelen moeten voldoen, terwijl de nieuwe regeling vanaf haar inwerkingtreding onmiddellijk van toepassing was op nieuwe vooraf betaalde kaarten.

B.8.7.2. In zoverre de verzoekende partijen de bestreden bepaling verwijten dat zij onvoldoende duidelijk maakt op welke categorieën van eindgebruikers van elektronische-communicatienetwerken zij van toepassing is, volstaat de vaststelling dat, conform de initiële doelstelling van artikel 127 van de wet van 13 juni 2005, alle eindgebruikers onder haar toepassingsgebied vallen, ongeacht of zij een abonnement of een vooraf betaalde belkaart hebben. Zoals in B.2.6 werd uiteengezet, is de gelijkschakeling van de eindgebruikers van een vooraf betaalde belkaart met de abonnementhouders overigens één van de doelstellingen van de bestreden wet.

B.8.7.3. In zoverre de verzoekende partijen de bestreden bepaling verwijten dat zij de omstandigheden van de gegevensverwerking niet preciseert, dient te worden vastgesteld dat zij in dat verband verwijst naar artikel 126, § 3, van de wet van 13 juni 2005.

Bij zijn arrest nr. 57/2021 van 22 april 2021 heeft het Hof onder meer artikel 4 van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie » vernietigd. Bij zijn arrest nr. 84/2015 van 11 juni 2015 had het Hof reeds de wet van 30 juli 2013 « houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering » vernietigd. Als gevolg van die arresten is artikel 126 van de wet van 13 juni 2005 thans van toepassing in de versie ervan die laatst werd gewijzigd bij artikel 33 van de wet van 4 februari 2010 « betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten ». De vermelde vernietigingen steunden in wezen op het verbod van een algemene en ongedifferentieerde bewaring van gegevens. Rekening houdend met de unierechtelijke grondslag van dat verbod, kan artikel 126 van de wet van 13 juni 2005 niet van toepassing worden geacht in de versie die aan die vernietigingen voorafgaat, in zoverre zij betrekking heeft op een algemene en ongedifferentieerde bewaring van gegevens inzake elektronische communicatie. Dezelfde bepaling kan echter wel worden toegepast in zoverre zij betrekking heeft op de identificatiegegevens van gebruikers van vooraf betaalde belkaarten bedoeld in artikel 127 van dezelfde wet. Artikel 126, zoals gewijzigd bij de wet van 4 februari 2010, bepaalt :

« § 1. Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de Minister van Justitie en van de minister en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de voorwaarden vast waaronder de operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

§ 2. De gegevens die moeten worden bewaard en de duur van de bewaring, die wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn, worden door de Koning bepaald in een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut.

De operatoren zorgen ervoor dat de in § 1 vermelde gegevens onbeperkt toegankelijk zijn vanuit België ».

Ter uitvoering van die bepaling regelt het koninklijk besluit van 19 september 2013 « tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie » (hierna : het koninklijk besluit van 19 september 2013) thans de verwerking en de bewaring van de persoonsgegevens, ook voor wat betreft de identificatiegegevens die worden verzameld op grond van artikel 127 van de wet van 13 juni 2005.

In zijn aanvullende memorie en ter terechtzitting heeft de Ministerraad er overigens op gewezen dat een nieuwe versie van artikel 126 van de wet van 13 juni 2005, om te voldoen aan de vereisten van het arrest van het Hof nr. 57/2021 en de daarin toegepaste rechtspraak van het Hof van Justitie, in voorbereiding is.

B.8.7.4. In zoverre de verzoekende partijen de bestreden bepaling verwijten dat zij niet regelt wie toegang heeft tot de bewaarde identificatiegegevens en op grond van welke voorwaarden, volstaat de vaststelling dat die toegang niet wordt geregeld door artikel 127 van de wet van 13 juni 2005, maar door de artikelen 46*bis*, 88*bis* en 90*ter* tot 90*decies* het Wetboek van strafvordering voor wat betreft de toegang in het kader van een strafrechtelijk onderzoek, door artikel 16/2, § 1, de wet van 30 november 1998 voor wat betreft de toegang door de inlichtingen- en veiligheidsdiensten en door artikel 107, § 2, van de wet van 13 juni 2005 voor wat betreft de toegang door de nooddiensten.

B.8.8. Bovendien kon de wetgever, door zulk een delegatie te verlenen, de Koning niet machtigen om bepalingen te nemen die zouden leiden tot een schending van het recht op eerbiediging van het privéleven. Het komt de bevoegde rechter toe na te gaan of de Koning op een al dan niet wettige wijze gebruik heeft gemaakt van de delegatie die Hem werd verleend.

B.9.1. Uit het voorgaande blijkt dat artikel 127 van de wet van 13 juni 2005, zoals gewijzigd bij artikel 2 van de bestreden wet, het wettigheidsbeginsel gewaarborgd door artikel 22 van de Grondwet schendt, zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen. In die mate dient artikel 2 van de bestreden wet te worden vernietigd.

Voor het overige is het eerste middel niet gegrond, aangezien de bestreden machtigingen aan de Koning betrekking hebben op de uitvoering van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn bepaald.

B.9.2. In tegenstelling tot wat de verzoekende partijen aanvoeren, heeft het Europees Hof voor de Rechten van de Mens bij zijn arrest-*Rotaru* niet geoordeeld dat de verwerking van persoonsgegevens en de toegang tot de verwerkte gegevens door de wetgevende macht dienen te worden geregeld. Het heeft slechts beklemtoond dat die verwerking en toegang een duidelijke, toegankelijke en voorzienbare basis in de interne regelgeving moeten hebben (EHRM, grote kamer, 4 mei 2000, *Rotaru t. Roemenië*, §§ 47-63).

Ook het Hof van Justitie vereist slechts dat « de rechtsgrond die de inmenging in [het recht op eerbiediging van het privéleven] toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen » (HvJ, 6 oktober 2020, C-623/17, *Privacy International*, punt 65). Het vereist niet dat alle aspecten van die beperking bij formele wet worden geregeld.

Een toetsing van de bestreden bepaling aan artikel 8 van het Europees verdrag voor de rechten van de mens, aan de artikelen 7 en 8 van het Handvest of aan artikel 5 van de AVG leidt bijgevolg niet tot een andere conclusie, aangezien uit die bepalingen geen strengere eisen inzake het formele wettigheidsbeginsel voortvloeien dan uit artikel 22 van de Grondwet.

B.9.3. Aangezien de vastgestelde schending slechts betrekking heeft op artikel 22 van de Grondwet, en niet op de in het middel aangevoerde normen van Europees Unierecht, staat het aan het Hof om, op grond van artikel 8, derde lid, van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, die gevolgen van de vernietigde bepalingen aan te wijzen welke als gehandhaafd moeten worden beschouwd of voorlopig gehandhaafd worden voor de termijn die het vaststelt.

De vastgestelde schending van artikel 22 van de Grondwet heeft geen betrekking op de aard en inhoud van de identificatiegegevens of identificatiedocumenten zoals die thans zijn geregeld in het koninklijk besluit van 27 november 2016 en die buiten de toetsingsbevoegdheid van het Hof vallen. Zij heeft slechts betrekking op het feit dat die gegevens en documenten in een wetskrachtige bepaling dienden te worden opgesomd.

Aan de wetgever moet bijgevolg de nodige tijd worden gegeven om in die wettelijke grondslag te voorzien, zonder dat in tussentijd de door de bestreden bepaling geregelde identificatie van de eindgebruikers van vooraf betaalde belkaarten dient te worden vernietigd. Die termijn dient bovendien voldoende lang te zijn om de wetgever toe te laten die wettelijke grondslag af te stemmen op de nieuwe dataretentieregeling die ingevolge het arrest van het Hof nr. 57/2021 van 22 april 2021 in voorbereiding is.

Bijgevolg dienen de gevolgen van de bestreden bepaling te worden gehandhaafd zoals aangegeven in het dictum.

Ten aanzien van het tweede middel

B.10. In het tweede middel voeren de verzoekende partijen aan dat de artikelen 2 en 3 van de bestreden wet de artikelen 10, 11, 19, 22 en 25 van de Grondwet, in samenhang gelezen met de artikelen 8 en 10 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11 en 52 van het Handvest, met de artikelen 56 en 57 van het Verdrag betreffende de werking van de Europese Unie, met de artikelen 2, *a)*, en 6 van de richtlijn 95/46/EG en met de artikelen 1, 2, 3, 5, 6, 9 en 15 van de richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 « betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) » schenden. Dit middel bestaat uit drie onderdelen.

B.11.1. Artikel 19 van de Grondwet bepaalt :

« De vrijheid van eredienst, de vrije openbare uitoefening ervan, alsmede de vrijheid om op elk gebied zijn mening te uiten, zijn gewaarborgd, behoudens bestraffing van de misdrijven die ter gelegenheid van het gebruikmaken van die vrijheden worden gepleegd ».

Artikel 25 van de Grondwet bepaalt :

« De drukpers is vrij; de censuur kan nooit worden ingevoerd; geen borgstelling kan worden geëist van de schrijvers, uitgevers of drukkers.

Wanneer de schrijver bekend is en zijn woonplaats in België heeft, kan de uitgever, de drukker of de verspreider niet worden vervolgd ».

Artikel 10 van het Europees Verdrag voor de rechten van de mens bepaalt :

« 1. Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of door te geven, zonder inmenging van overheidswege en ongeacht grenzen. Dit artikel belet niet dat Staten radio-omroep-, bioscoop- of televisie-ondernemingen kunnen onderwerpen aan een systeem van vergunningen.

2. Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, welke bij de wet worden voorzien en die in een democratische samenleving nodig zijn in het belang van 's land veiligheid, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechtelijke macht te waarborgen ».

Artikel 11 van het Handvest bepaalt :

« 1. Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te hebben en de vrijheid kennis te nemen en te geven van informatie of ideeën, zonder inmenging van enig openbaar gezag en ongeacht grenzen.

2. De vrijheid en de pluriformiteit van de media worden geëerbiedigd ».

In zoverre het recht op vrijheid van meningsuiting daarin wordt erkend, hebben artikel 10 van het Europees Verdrag voor de rechten van de mens en artikel 11, lid 1, van het Handvest een draagwijdte die analoog is aan die van artikel 19 van de Grondwet, waarin de vrijheid om op elk gebied zijn mening te uiten, wordt erkend.

De door die bepalingen verstrekte waarborgen vormen in die mate dan ook een onlosmakelijk geheel.

B.11.2. Artikel 56 van het Verdrag betreffende de werking van de Europese Unie bepaalt :

« In het kader van de volgende bepalingen zijn de beperkingen op het vrij verrichten van diensten binnen de Unie verboden ten aanzien van de onderdanen der lidstaten die in een andere lidstaat zijn gevestigd dan die, waarin degene is gevestigd te wiens behoeve de dienst wordt verricht.

Het Europees Parlement en de Raad kunnen, volgens de gewone wetgevingsprocedure, de bepalingen van dit hoofdstuk van toepassing verklaren ten gunste van de onderdanen van een derde staat die diensten verrichten en binnen de Unie zijn gevestigd ».

Artikel 57 van het Verdrag betreffende de werking van de Europese Unie bepaalt :

« In de zin van de Verdragen worden als diensten beschouwd de dienstverrichtingen welke gewoonlijk tegen vergoeding geschieden, voor zover de bepalingen, betreffende het vrije verkeer van goederen, kapitaal en personen op deze dienstverrichtingen niet van toepassing zijn.

De diensten omvatten met name werkzaamheden :

a) van industriële aard,

b) van commerciële aard,

c) van het ambacht,

d) van de vrije beroepen.

Onverminderd de bepalingen van het hoofdstuk betreffende het recht van vestiging, kan degene die de diensten verricht, daartoe zijn werkzaamheden tijdelijk uitoefenen in de lidstaat waar de dienst wordt verricht, onder dezelfde voorwaarden als die welke die staat aan zijn eigen onderdanen oplegt ».

B.11.3. De artikelen 1, 2, 3, 5, 6, 9 en 15 van de richtlijn 2002/58/EG bepalen :

« Artikel 1. Werkingssfeer en doelstelling

1. Deze richtlijn voorziet in de harmonisering van de regelgeving van de lidstaten die nodig is om een gelijk niveau van bescherming van fundamentele rechten en vrijheden - met name het recht op een persoonlijke levenssfeer en vertrouwelijkheid - bij de verwerking van persoonsgegevens in de sector elektronische communicatie te waarborgen en om te zorgen voor het vrij verkeer van dergelijke gegevens en van elektronischecommunicatieapparatuur en -diensten in de Gemeenschap.

2. Voor op de doelstellingen van lid 1 vormen de bepalingen van deze richtlijn een specificatie van en een aanvulling op Richtlijn 95/46/EG. Bovendien voorzien zij in bescherming van de rechtmatige belangen van abonnees die rechtspersonen zijn.

3. Deze richtlijn is niet van toepassing op activiteiten die niet onder het EG-Verdrag vallen, zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie, en in geen geval op activiteiten die verband houden met de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economische welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de activiteiten van de staat op strafrechtelijk gebied.

Artikel 2. Definities

Tenzij anders is bepaald, zijn de definities van Richtlijn 95/46/EG van het Europees Parlement en de Raad en Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (kaderrichtlijn) van toepassing.

Daarnaast wordt in deze richtlijn verstaan onder :

a) ' gebruiker ' : natuurlijke persoon die gebruikmaakt van een openbare elektronische-communicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd;

b) ' verkeersgegevens ' : gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan;

c) ' locatiegegevens ' : gegevens die in een elektronischecommunicatienetwerk of door een elektronische-communicatiedienst worden verwerkt, waarmee de geografische positie van de eindapparatuur van een gebruiker van een openbare elektronischecommunicatiedienst wordt aangegeven;

d) ' communicatie ' : informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronische-communicatiedienst. Dit omvat niet de informatie die via een omroepdienst over een elektronische-communicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gerelateerd aan de identificeerbare abonnee of gebruiker die de informatie ontvangt;

f) ' toestemming ' van een gebruiker of abonnee : toestemming van de betrokkene in de zin van Richtlijn 95/46/EG;

g) ' dienst met toegevoegde waarde ' : dienst die de verwerking vereist van verkeersgegevens of locatiegegevens anders dan verkeersgegevens, en die verder gaat dan hetgeen nodig is voor het overbrengen van een communicatie of de facturering ervan;

h) ' e-mail ' : tekst-, spraak-, geluids- of beeldbericht dat over een openbaar communicatienetwerk wordt verzonden en in het netwerk of in de eindapparatuur van de ontvanger kan worden opgeslagen tot het door de ontvanger wordt opgehaald;

i) ' inbreuk in verband met persoonsgegevens ' : een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronischecommunicatiedienst in de Gemeenschap.

Artikel 3. Betrokken diensten

Deze richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de Gemeenschap, met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen.

[...]

Artikel 5. Vertrouwelijk karakter van de communicatie

1. De lidstaten garanderen via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische-communicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1. Dit lid laat de technische opslag die nodig is voor het overbrengen van informatie onverlet, onverminderd het vertrouwelijkheidsbeginsel.

2. Lid 1 laat de bij de wet toegestane registratie van communicatie en de daarmee verband houdende verkeersgegevens onverlet, wanneer die wordt uitgevoerd in het legale zakelijke verkeer ten bewijze van een commerciële transactie of van enigerlei andere zakelijke communicatie.

3. De lidstaten dragen ervoor zorg dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig Richtlijn 95/46/EG, onder meer over de doeleinden van de verwerking. Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert.

Artikel 6. Verkeersgegevens

1. Verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronische-communicatienetwerk of -dienst, moeten, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, worden gewist of anoniem gemaakt, onverminderd de leden 2, 3 en 5, alsmede artikel 15, lid 1.

2. Verkeersgegevens die noodzakelijk zijn ten behoeve van de facturering van abonnees en interconnectie-betalingen mogen worden verwerkt. Die verwerking is slechts toegestaan tot aan het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen.

3. De aanbieder van een openbare elektronischecommunicatiedienst mag ten behoeve van de marketing van elektronischecommunicatiediensten of voor de levering van diensten met toegevoegde waarde de in lid 1 bedoelde gegevens verwerken voor zover en voor zolang dat nodig is voor dergelijke diensten of marketing, indien de abonnee of de gebruiker waarop de gegevens betrekking hebben daartoe zijn voorafgaande toestemming heeft gegeven. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.

4. De dienstenaanbieder moet de abonnee of gebruiker in kennis stellen van de soorten verkeersgegevens die worden verwerkt en van de duur van de verwerking voor de in lid 2 genoemde doeleinden en, voorafgaand aan het verkrijgen van diens toestemming, voor de in lid 3 genoemde doeleinden.

5. De verwerking van verkeersgegevens overeenkomstig de leden 1 tot en met 4 mag alleen worden uitgevoerd door personen die werkzaam zijn onder het gezag van de aanbieders van de openbare communicatienetwerken of -diensten voor facturering of verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude en marketing van elektronische-communicatiediensten van de aanbieder of de levering van diensten met toegevoegde waarde, en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren.

6. De leden 1, 2, 3 en 5 zijn van toepassing onverminderd de mogelijkheid voor de bevoegde organen om overeenkomstig de toepasselijke wetgeving in kennis te worden gesteld van verkeersgegevens met het oog op het beslechten van geschillen, in het bijzonder met betrekking tot interconnectie en facturering.

[...]

Artikel 9. Andere locatiegegevens dan verkeersgegevens

1. Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronische-communicatienetwerken of -diensten verwerkt kunnen worden, mogen deze gegevens slechts worden verwerkt wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voorzover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. De dienstenaanbieder moet de gebruikers of abonnees, voorafgaand aan het verkrijgen van hun toestemming, in kennis stellen van de soort locatiegegevens anders dan verkeersgegevens, die zullen worden verwerkt, en van de doeleinden en de duur van die verwerking, en hun meedelen of deze gegevens aan een derde zullen worden doorgegeven ten behoeve van de levering van de dienst met toegevoegde waarde. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van andere locatiegegevens dan verkeersgegevens te allen tijde intrekken.

2. Wanneer de gebruikers of abonnees toestemming hebben gegeven voor de verwerking van andere locatiegegevens dan verkeersgegevens, moet de gebruiker of abonnee de mogelijkheid behouden om op eenvoudige en kosteloze wijze tijdelijk de verwerking van dergelijke gegevens te weigeren voor elke verbinding met het netwerk of voor elke transmissie van communicatie.

3. De verwerking van locatiegegevens anders dan verkeersgegevens in overeenstemming met de leden 1 en 2, moet worden beperkt tot personen die werkzaam zijn onder het gezag van de aanbieder van het openbare elektronische-communicatienetwerk of de openbare elektronische-communicatiedienst of de derde die de dienst met toegevoegde waarde levert, en moet beperkt blijven tot hetgeen noodzakelijk is om de dienst met toegevoegde waarde te kunnen aanbieden.

[...]

Artikel 15. Toepassing van een aantal bepalingen van Richtlijn 95/46/EG

1. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.

1*bis*. Lid 1 is niet van toepassing op de uit hoofde van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatie-netwerken (4) te bewaren gegevens voor de in artikel 1, lid 1, van die richtlijn bedoelde doeleinden.

1*ter*. Aanbieders zetten interne procedures op voor de afhandeling van verzoeken om toegang tot persoons-gegevens van gebruikers op de grondslag van nationale bepalingen die overeenkomstig lid 1 zijn aangenomen. Zij verstrekken aan de bevoegde nationale instantie op verzoek gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en hun antwoord.

2. Het bepaalde in hoofdstuk III van Richtlijn 95/46/EG inzake beroep op de rechter, aansprakelijkheid en sancties geldt voor de nationale bepalingen die uit hoofde van deze richtlijn worden aangenomen en ten aanzien van de individuele rechten die uit deze richtlijn voortvloeien.

3. De Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, ingesteld bij artikel 29 van Richtlijn 95/46/EG, voert de in artikel 30 van die richtlijn vermelde taken ook uit ten aanzien van aangelegenheden die onder de onderhavige richtlijn vallen, namelijk de bescherming van de fundamentele rechten en vrijheden en van rechtmatige belangen in de sector elektronische communicatie ».

Wat betreft het eerste onderdeel van het tweede middel

B.12. In het eerste onderdeel van het tweede middel voeren de verzoekende partijen aan dat de algemene en ongedifferentieerde identificatieplicht voor alle eindgebruikers van elektronische-communicatiediensten die de bestreden wet in het leven roept, een inmenging in het recht op eerbiediging van het privéleven uitmaakt die verder gaat dan noodzakelijk in het licht van de nagestreefde doelstellingen.

B.13.1. Het recht op eerbiediging van het privéleven is niet absoluut. De aangehaalde grondwets- en verdragsbepalingen sluiten een overheidsinmenging in het recht op eerbiediging van het privéleven niet uit, maar vereisen dat zij wordt toegestaan door een voldoende precieze wettelijke bepaling, dat zij beantwoordt aan een dwingende maatschappelijke behoefte in een democratische samenleving en dat zij evenredig is met de daarmee nagestreefde wettige doelstelling.

De wetgever beschikt ter zake over een appreciatiemarge. Die appreciatiemarge is evenwel niet onbegrensd : opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat de wetgever een billijk evenwicht heeft gevonden tussen alle rechten en belangen die in het geding zijn. Bij de beoordeling van dat evenwicht houdt het Europees Hof voor de Rechten van de Mens onder meer rekening met de bepalingen van het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens en de aanbeveling nr. R (87) 15 van het Comité van Ministers aan de verdragsstaten tot regeling van het gebruik van persoonsgegevens in de politiesector (EHRM, 25 februari 1997, *Z t. Finland*, § 95; grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, § 103).

B.13.2. Bij de beoordeling van de evenredigheid van maatregelen met betrekking tot de verwerking van persoonsgegevens, dient rekening te worden gehouden met, onder meer, het geautomatiseerde karakter ervan, de gebruikte technieken, de accuraatheid, de pertinentie en het al dan niet buitensporige karakter van de gegevens die worden verwerkt, het al dan niet voorhanden zijn van maatregelen die de duur van de bewaring van de gegevens beperken, het al dan niet voorhanden zijn van een systeem van onafhankelijk toezicht dat toelaat na te gaan of de bewaring van de gegevens nog langer is vereist, het al dan niet voorhanden zijn van afdoende controlerechten en rechtsmiddelen voor de betrokkenen, het al dan niet voorhanden zijn van waarborgen ter voorkoming van stigmatisering van de personen van wie de gegevens worden verwerkt, het onderscheidend karakter van de regeling en het al dan niet voorhanden zijn van waarborgen ter voorkoming van foutief gebruik en misbruik van de verwerkte persoonsgegevens door de overheidsdiensten (arrest nr. 108/2016 van 14 juli 2016, B.12.2; arrest nr. 29/2018 van 15 maart 2018, B.14.4; arrest nr. 27/2020 van 20 februari 2020, B.8.3; EHRM, grote kamer, 4 mei 2000, *Rotaru t. Roemenië*, § 59; beslissing, 29 juni 2006, *Weber en Saravia t. Duitsland*, § 135; 28 april 2009, *K.H. e.a. t. Slowakije*, §§ 60-69; grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, §§ 101-103, 119, 122 en 124; 18 april 2013, *M.K. t. Frankrijk*, §§ 37 en 42-44; 18 september 2014, *Brunet t. Frankrijk*, §§ 35-37; 12 januari 2016, *Szabó en Vissy t. Hongarije*, § 68; 30 januari 2020, *Breyer t. Duitsland*, §§ 73-80; grote kamer, 25 mei 2021, *Centrum för rättvisa t. Zweden*, §§ 262-278; grote kamer, 25 mei 2021, *Big Brother Watch t. Verenigd Koninkrijk*, §§ 348-364; HvJ, grote kamer, 8 april 2014, C-293/12, *Digital Rights Ireland Ltd*, en C-594/12, *Kärntner Landesregierung e.a.*, punten 56-66; grote kamer, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, punten 105-133; grote kamer, 6 oktober 2020, C-623/17, *Privacy International*, punten 58-82; grote kamer, 2 maart 2021, C-746/18, *Prokuratuur*, punten 50-56).

B.13.3. Uit de rechtspraak van het Europees Hof voor de Rechten van de Mens blijkt dat persoonsgegevens niet langer dan nodig voor de verwezenlijking van het doel waarvoor ze werden opgeslagen, mogen worden bewaard in een vorm die identificatie toelaat of die toelaat een verband te leggen tussen een persoon en strafbare feiten. Bij de beoordeling van de evenredigheid van de duur van bewaring ten aanzien van het doel waarvoor de gegevens werden opgeslagen, houdt het Europees Hof voor de Rechten van de Mens rekening met het al dan niet bestaan van een onafhankelijk toezicht op de verantwoording voor het behoud van gegevens in de databanken aan de hand van duidelijke criteria, zoals de ernst van de feiten, het feit dat de betrokken persoon vroeger reeds het voorwerp is geweest van een aanhouding, de ernst van de verdenkingen die rusten op een persoon, en elke andere bijzondere omstandigheid (EHRM, grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, § 103; 18 april 2013, *M.K. t. Frankrijk*, § 35; 17 december 2009, *B.B. t. Frankrijk*, § 61; 18 september 2014, *Brunet t. Frankrijk*, §§ 35-40).

B.14.1. Wat de algemene en ongedifferentieerde verzameling, verwerking en bewaring van persoonsgegevens van de gebruikers van elektronische-communicatienetwerken betreft, maken zowel het Europees Hof voor de Rechten van de Mens als het Hof van Justitie een onderscheid tussen, enerzijds, verkeers- en locatiegegevens en, anderzijds, identificatiegegevens.

B.14.2. Zij beschouwen de verzameling, verwerking en bewaring van verkeers- en locatiegegevens van die gebruikers als een zeer ernstige beperking van het recht op eerbiediging van het privéleven, aangezien dergelijke gegevens gevoelige informatie kunnen vrijgeven over een groot aantal aspecten van het privéleven van de betrokken personen, zoals hun seksuele geaardheid, politieke opvattingen, religieuze, filosofische, maatschappelijke of andersoortige overtuigingen en gezondheid.

Uit dergelijke gegevens kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie zij worden bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, hun activiteiten, hun sociale relaties en de sociale kringen waarin zij verkeren. Dergelijke informatie maakt het mogelijk een profiel van de betrokken personen op te stellen, hetgeen even gevoelig is als de inhoud zelf van de communicatie (EHRM, grote kamer, 25 mei 2021, *Centrum för rättvisa t. Zweden*, §§ 238-245; grote kamer, 25 mei 2021, *Big Brother Watch t. Verenigd Koninkrijk*, §§ 324-331; HvJ, grote kamer, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, punt 117; grote kamer, 6 oktober 2020, C-623/17, *Privacy International*, punt 71).

Het Hof van Justitie leidt daaruit af dat de algemene en ongedifferentieerde verzameling, verwerking en bewaring van verkeers- en locatiegegevens in beginsel verboden is. Zij is slechts toegestaan om redenen van nationale veiligheid, en slechts in zoverre er voldoende concrete aanwijzingen zijn dat de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging van de nationale veiligheid en dat die bedreiging werkelijk, actueel en voorzienbaar is. Bovendien mag die bewaring niet langer duren dan strikt noodzakelijk in het licht van die bedreiging van de nationale veiligheid en moet zij zijn omgeven met strikte waarborgen die ervoor zorgen dat de persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik, onder meer aan de hand van een effectieve toetsing door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit (HvJ, grote kamer, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, punten 137-139). Een verzameling, verwerking en bewaring van verkeers- en locatiegegevens met het oog op de bestrijding van ernstige criminaliteit mag daarentegen geen algemeen en ongedifferentieerd karakter hebben, maar dient op geografische of persoonsgebonden basis te worden afgebakend (*ibid.*, punten 144-150).

Het Europees Hof voor de Rechten van de Mens verbiedt daarentegen niet de algemene en ongedifferentieerde verzameling, verwerking en bewaring van verkeers- en locatiegegevens, maar onderwerpt deze aan een strikte toetsing. Het beoordeelt de wettigheid en de noodzaak in een democratische samenleving van dergelijke maatregelen aan de hand van de reden waarom de « bulkinterceptie » wordt bevolen, de omstandigheden waarin de communicatie van private personen wordt onderschept, de procedure waarmee toelating voor de bulkinterceptie wordt gegeven, de procedure waarmee het te gebruiken materiaal wordt gekozen, de voorzorgen die worden genomen indien de verwerkte gegevens aan derden worden gecommuniceerd, de tijdslimiet waaraan het onderscheppen en bewaren van persoonsgegevens wordt onderworpen, met inbegrip van de omstandigheden waarin de gegevens worden vernietigd, de procedure en de modaliteiten van het toezicht *a priori* door een onafhankelijke instantie op de naleving van de waarborgen, met inbegrip van het door die instantie geboden rechtsherstel, en de procedure van de onafhankelijke toetsing *a posteriori* van de naleving van alle toepasselijke regels (EHRM, grote kamer, 25 mei 2021, *Centrum för rättvisa t. Zweden*, § 275; grote kamer, 25 mei 2021, *Big Brother Watch t. Verenigd Koninkrijk*, § 361).

B.14.3. Daarentegen beschouwen het Europees Hof voor de Rechten van de Mens en het Hof van Justitie de algemene en ongedifferentieerde verzameling, verwerking en bewaring van loutere identificatiegegevens van gebruikers van elektronische-communicatienetwerken als een minder ernstige beperking van het recht op eerbiediging van het privéleven, omdat met die gegevens alleen noch de datum, het tijdstip, de duur en de ontvangers van een communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal

malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Die gegevens verschaffen dus geen informatie over wat die personen hebben gecommuniceerd, noch over hun privéleven. Aan de hand van die gegevens alleen kan geen profiel van de gebruiker worden opgesteld of kunnen zijn bewegingen niet worden gevolgd (EHRM 30 januari 2020, *Breyer t. Duitsland*, §§ 92-95; HvJ, 2 oktober 2018, C-207/16, *Ministerio Fiscal*, punt 62; grote kamer, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, punt 157).

Het Hof van Justitie leidt daaruit af dat het recht op eerbied voor het privéleven zich niet verzet tegen een algemene en ongedifferentieerde verzameling, verwerking en bewaring van identificatiegegevens van gebruikers van elektronische-communicatienetwerken ten behoeve van het onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid. Het hoeft daarbij niet te gaan om ernstige strafbare feiten of om ernstige bedreigingen en verstoringen van de openbare veiligheid (HvJ, grote kamer, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, punt 159). Wel dient te worden aangetoond dat « die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik » (*ibid.*, punt 168).

Het Europees Hof voor de Rechten van de Mens toetst de algemene en ongedifferentieerde verzameling, verwerking en bewaring van die identificatiegegevens op minder intensieve wijze dan de verzameling, verwerking en bewaring van verkeers- en locatiegegevens. Het gaat allereerst na of de bewaartermijn redelijk is, rekening houdend met de gebruikelijke duur van een strafrechtelijk onderzoek. Wat de toegang tot de bewaarde identificatiegegevens betreft, vereist het dat de autoriteiten die de gegevens kunnen raadplegen, limitatief in de toepasselijke regelgeving worden opgesomd, dat hun toegang gebaseerd is op een specifieke en duidelijke wettelijke basis in het strafprocesrecht of in de wetgeving op de inlichtingen- en veiligheidsdiensten en dat zij wordt verantwoord door een initiële concrete verdenking. Zodra de overheid de opgevraagde identificatiegegevens niet langer nodig heeft, dient zij die onmiddellijk te vernietigen. Het Europees Hof voor de Rechten van de Mens vereist niet dat de betrokkene wordt ingelicht over de toegang tot zijn identificatiegegevens. Het vereist evenmin dat er voor de toegang tot loutere identificatiegegevens een toezicht *a priori* wordt ingesteld : een toegang *a posteriori* tot een onafhankelijke rechterlijke of bestuurlijke instantie, in samenhang met de gemeenrechtelijke rechtsmiddelen waarover de verdachte tijdens een strafproces beschikt, volstaat (EHRM, 30 januari 2020, *Breyer t. Duitsland*, §§ 96-107).

B.15.1. Bij zijn arrest nr. 57/2021 van 22 april 2021 heeft het Hof de artikelen 2, *b)*, 3 tot 11 en 14 van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie » vernietigd omdat daarin een algemene en ongedifferentieerde verzameling, verwerking en bewaring van zowel identificatiegegevens als verkeers- en locatiegegevens werd geregeld. Het Hof stelde vast « dat de bestreden wet, wat het beginsel zelf ervan betreft, [berustte] op een verplichting tot algemene en ongedifferentieerde bewaring van alle gegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, en dat zij, in het algemeen [...] ruimere doelstellingen [nastreefde] dan de bestrijding van zware criminaliteit of het risico van aantasting van de openbare veiligheid » (B.17). De bestreden wet waarborgde bovendien niet dat de verzameling, verwerking en bewaring van gegevens met betrekking tot de elektronische communicatie de uitzondering in plaats van de regel was, noch dat de toegang tot die gegevens was onderworpen aan duidelijke en nauwkeurige regels, dat de inmenging in het recht op eerbiediging van het privéleven tot het strikt noodzakelijke werd beperkt en dat elke inmenging beantwoordde aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel (B.18).

B.15.2. De thans bestreden wet heeft daarentegen slechts betrekking op de in artikel 127 van de wet van 13 juni 2005 bedoelde gegevens aan de hand waarvan de eindgebruiker van een elektronische-communicatiedienst die wordt geleverd op basis van een vooraf betaalde belkaart kan worden geïdentificeerd. Artikel 12, tweede lid, van het koninklijk besluit van 27 november 2016 bepaalt dat die identificatiegegevens kunnen verschillen afhankelijk van de gekozen identificatiemethode, maar somt tevens op limitatieve wijze de identificatiegegevens op die de betrokken onderneming maximaal mag bewaren :

« 1° de naam en voornaam;

2° het geslacht;

3° de nationaliteit;

4° de geboorteplaats en -datum;

5° het adres van de woonplaats, het e-mailadres en het telefoonnummer;

6° het rijksregisternummer;

7° het nummer van het identiteitsstuk, het land van uitgifte van het document wanneer het een buitenlands document betreft en de geldigheidsdatum van het document;

8° de referenties van de betalingstransactie, conform artikel 17;

9° het verband van de voorafbetaalde kaart met het product waarvoor de eindgebruiker reeds geïdentificeerd is, conform artikel 18;

10° de foto van de eindgebruiker, maar enkel voor andere documenten dan de Belgische elektronische identiteitskaart ».

Gelet op de gedeeltelijke vernietiging bedoeld in B.9.1 en de handhaving van de gevolgen bedoeld in B.9.3 dient de wetgever vóór de datum vermeld in het dictum de identificatiegegevens en identificatiedocumenten die voor de toepassing van artikel 127 van de wet van 13 juni 2005 kunnen dienen, in een wetsbepaling op te nemen.

B.15.3. Die persoonsgegevens zijn geen verkeers- en locatiegegevens, maar slechts de gegevens die gewoonlijk worden gehanteerd om iemand te identificeren. Het is niet mogelijk om aan de hand van die gegevens alleen iemands verplaatsingen, communicaties, activiteiten of sociale relaties te volgen, noch om een persoonlijk profiel op te stellen dat toelaat precieze conclusies te trekken over iemands seksuele geaardheid, overtuigingen en gezondheid. Zij geven op zich dus geen gevoelige informatie over het privéleven prijs.

Het is juist dat die identificatiegegevens vervolgens kunnen worden gekoppeld aan andere gegevens en op die manier kunnen bijdragen aan het vrijgeven van dergelijke gevoelige informatie over iemands privéleven. Die andere gegevens dienen dan evenwel op een andere manier te worden verzameld, en ook die verzameling dient te geschieden met eerbied voor de toepasselijke wetgeving en voor de grondrechten van de betrokkene.

Bijgevolg dient de bestaanbaarheid van de bestreden wet met het recht op eerbiediging van het privéleven te worden beoordeeld aan de hand van de in B.14.3 vermelde criteria.

B.16.1. De materiële en procedurele voorwaarden voor de verzameling, verwerking en bewaring van de identificatiegegevens van eindgebruikers van een elektronische-communicatienetwerk op basis van een vooraf betaalde belkaart worden geregeld in de artikelen 126 en 127 van de wet van 13 juni 2005 en in de koninklijke besluiten van 19 september 2013 en 27 november 2016.

B.16.2. Zoals uiteengezet in B.2.1 tot B.2.7 bepaalt artikel 127 van de wet van 13 juni 2005 aan welke personen in dit kader verplichtingen worden opgelegd, namelijk aan de operatoren, de aanbieders, de verkoopkanalen van elektronische-communicatiediensten, de ondernemingen die een identificatiedienst verstrekken en de eindgebruikers zelf. Het duidt tevens de bevoegde gegevensverwerker aan, namelijk de operator of de aanbieder. Het bepaalt voorts het beginsel dat alle eindgebruikers identificeerbaar dienen te zijn, ongeacht of zij een oude dan wel een nieuwe vooraf betaalde belkaart gebruiken, alsook dat de identificatie dient te gebeuren op grond van een identificatiedocument waarop het rijksregisternummer staat.

Het koninklijk besluit van 27 november 2016 verplicht de eindgebruikers van vooraf betaalde belkaarten om zich uiterlijk bij de activering ervan bij de operator te identificeren volgens één van de in hetzelfde koninklijk besluit beschreven geldige identificatiemethodes en aan de hand van één van de in het koninklijk besluit vermelde geldige identificatiedocumenten. Het verplichtte de operatoren om alle eindgebruikers van oude vooraf betaalde belkaarten te identificeren vóór 7 juni 2017 en verbiedt hun om nog nieuwe vooraf betaalde kaarten activeren indien de eindgebruiker nog niet is geïdentificeerd. Indien zij door de eindgebruiker worden verwittigd van het verlies of de diefstal van de vooraf betaalde belkaart, dienen zij die onmiddellijk onbruikbaar te maken.

Wat de eigenlijke gegevensverwerking betreft, bepaalt het koninklijk besluit van 27 november 2016 dat de operator, de leverancier van een identificatiedienst of het verkoopkanaal van elektronische-communicatiediensten de Belgische elektronische identiteitskaart via elektronische weg lezen, deze scannen of er een kopie of foto van maken, met inbegrip van de foto op die kaart en het nummer van die kaart. De operator dient vóór de activering van de vooraf betaalde belkaart te controleren of de voorgelegde identiteitskaart is gestolen of het voorwerp uitmaakt van fraude. Hij dient tevens de identificatiemethode die werd gebruikt om de eindgebruiker te identificeren, te bewaren gedurende de termijn bedoeld in artikel 126 van de wet van 13 juni 2005.

B.16.3. De verzoekende partijen betwisten niet dat die regels duidelijk en nauwkeurig zijn. Zij voeren slechts aan dat het wettelijke kader inzake de verdere bewaring van de verwerkte gegevens sinds het arrest van het Hof nr. 57/2021 van 22 april 2021 onduidelijk is, omdat het Hof in dat arrest de regels inzake de verwerkte gegevens, de bij de verwerking betrokken personen, de voorwaarden voor en de doeleinden van de verwerking, alsook de regels met betrekking tot de Coördinatiecel heeft vernietigd. Daardoor zouden er geen materiële en procedurele voorwaarden meer bestaan die de verwerking van de bewaarde identificatiegegevens of -documenten regelen.

B.16.4. Zoals uiteengezet in B.8.7.3, heeft het arrest nr. 57/2021 niet als gevolg dat er niet langer een wetgevend kader voor de bewaring van de verzamelde en verwerkte identificatiegegevens bestaat. De vernietiging van de artikelen 2, *b)*, 3 tot 11 en 14 van de wet van 29 mei 2016 heeft slechts als gevolg dat artikel 126 van de wet van 13 juni 2005 thans van toepassing is, wat de identificatiegegevens van gebruikers van vooraf betaalde belkaarten betreft, in de versie ervan die laatst werd gewijzigd bij artikel 33 van de wet van 4 februari 2010 « betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten ».

B.16.5. Ter uitvoering van artikel 126 van de wet van 13 juni 2005 bepaalt het koninklijk besluit van 19 september 2013 de voorwaarden voor de bewaring van de verzamelde gegevens. De artikelen 3 tot 6 van dat besluit bepalen welke gegevens dienen te worden bewaard en wie voor de bewaring instaat :

« Art. 3. § 1. Wat betreft de gegevens voor de identificatie van de eindgebruiker, van de eindapparatuur die vermoed wordt te zijn gebruikt en van de gebruikte elektronische-communicatiedienst, bewaren de aanbieders van openbare diensten voor vaste telefonie en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° het aan de eindgebruiker toegewezen nummer;

2° de persoonsgegevens van de eindgebruiker;

3° de datum van aanvang van het abonnement of van de registratie voor de dienst;

4° het soort van gebruikte vaste-telefoniedienst alsook de andere soorten van gebruikte diensten waarop de eindgebruiker ingeschreven heeft;

5° in geval van overdracht van het nummer van de eindgebruiker naar een andere operator, de identiteit van de aanbieder die het nummer en de identiteit overdraagt van de aanbieder naar wie het nummer wordt overgedragen;

6° de gegevens betreffende betalingswijze, identificatie van het betalingsmiddel en tijdstip van betaling voor het abonnement of voor het gebruik van de dienst.

§ 2. Wat de verkeers- en locatiegegevens betreft, bewaren de aanbieders van openbare diensten voor vaste telefonie en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie de volgende gegevens :

1° de identificatie van het telefoonnummer van de oproeper en van de opgeroepene;

2° de plaats van het netwerkaansluitpunt van de oproeper en van de opgeroepene;

3° in geval van een groepsgesprek, oproepdoorschakeling of -doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;

4° de datum en het juiste tijdstip van aanvang en einde van de oproep;

5° de beschrijving van de gebruikte telefoniedienst.

§ 3. De in paragraaf 1 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, eerste lid, van de wet.

De in paragraaf 2 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, tweede lid, van de wet.

Art. 4. § 1. Wat betreft de gegevens voor de identificatie van de eindgebruiker, van de eindapparatuur die vermoed wordt te zijn gebruikt en van de gebruikte elektronische-communicatiedienst, bewaren de aanbieders van een openbare dienst voor mobiele telefonie en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° het aan de eindgebruiker toegewezen nummer alsook de internationale identiteit van de mobiele abonnee (' International Mobile Subscriber Identity ', ' IMSI ');

2° de persoonsgegevens van de eindgebruiker;

3° de datum en de plaats van inschrijving op het abonnement of de registratie van de eindgebruiker;

4° de datum en het tijdstip van de eerste activering van de dienst, alsook de celidentiteit van waaruit de dienst is geactiveerd;

5° de aanvullende diensten waarop de eindgebruiker heeft ingetekend;

6° in geval van nummeroverdracht naar een andere operator, de identiteit van de operator vanwaar de eindgebruiker komt;

7° de gegevens betreffende betalingswijze, identificatie van het betaalmiddel en tijdstip van de betaling voor het abonnement of voor het gebruik van de dienst;

8° het identificatienummer van het mobiele eindtoestel van de eindgebruiker (' International Mobile Equipment Identity ', ' IMEI ').

§ 2. Wat de verkeers- en locatiegegevens betreft, bewaren de aanbieders van een openbare dienst voor mobiele telefonie en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° de identificatie van het telefoonnummer van de oproeper en van de opgeroepene;

2° in geval van een groepsgesprek, oproepdoorschakeling of -doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;

3° de ' International Mobile Subscriber Identity ' (' IMSI ') van de oproepende en opgeroepen deelnemer;

4° de ' International Mobile Equipment Identity ' (' IMEI ') van het mobiele eindapparaat van de oproepende en opgeroepen deelnemer;

5° de datum en het juiste tijdstip van aanvang en einde van de oproep;

6° de locatie van het netwerkaansluitpunt bij aanvang en bij het einde van elke verbinding;

7° de gegevens voor het identificeren van de geografische locatie van cellen middels referentie aan hun celidentiteit op het ogenblik dat de verbinding is gemaakt;

8° de technische karakteristieken van de gebruikte telefoondienst.

§ 3. De in paragraaf 1 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, eerste lid, van de wet.

De in paragraaf 2 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, tweede lid, van de wet.

Art. 5. § 1. Wat betreft de gegevens in verband met de identificatie van de eindgebruiker, van de eindapparatuur die vermoed wordt te zijn gebruikt en van de gebruikte elektronische-communicatiedienst, bewaren de aanbieders van openbare internettoegangsdiensten en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° de toegewezen eindgebruikersidentificatie;

2° de persoonsgegevens van de eindgebruiker;

3° de datum en het tijdstip van het nemen van het abonnement of de registratie van de eindgebruiker;

4° het IP-adres en de bronpoort van de verbinding die gediend hebben voor het nemen van het abonnement of voor de registratie van de eindgebruiker;

5° de identificatie van het netwerkaansluitpunt dat gediend heeft voor het nemen van het abonnement of voor de inschrijving als eindgebruiker;

6° de aanvullende diensten waarop de eindgebruiker ingeschreven heeft bij de betrokken aanbieder van openbare internettoegang;

7° de gegevens betreffende betalingswijze, identificatie van het betaalmiddel en tijdstip van de betaling voor het abonnement of voor het gebruik van de dienst.

§ 2. Wat de verkeers- en locatiegegevens betreft, bewaren de aanbieders van openbare internettoegangsdiensten en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° de eindgebruikersidentificatie;

2° *a)* het IP-adres;

b) in geval van het gedeelde gebruik van een IP-adres, de toegewezen poorten van het IP-adres evenals de datum en het uur van de toewijzing;

3° de identificatie en de locatie van het netwerkaansluitpunt dat door de eindgebruiker wordt gebruikt bij aanvang en bij het einde van een verbinding;

4° de datum en het tijdstip van de log-in en log-off van een sessie van de internettoegangsdienst;

5° het tijdens de sessie of een ander opgevraagde tijdseenheid geüploade en gedownloade volume van gegevens;

6° de gegevens voor het identificeren van de geografische locatie van cellen middels referentie aan hun celidentiteit op het ogenblik dat de verbinding is gemaakt.

§ 3. De in paragraaf 1 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, eerste lid, van de wet.

De in paragraaf 2 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, tweede lid, van de wet.

Art. 6. § 1. Wat betreft de gegevens voor de identificatie van de eindgebruiker, van de eindapparatuur die vermoed wordt te zijn gebruikt en van de gebruikte elektronische-communicatiedienst, bewaren de aanbieders van een openbare e-maildienst via internet, de aanbieders van een openbare internettelefoniedienst en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° de eindgebruikersidentificatie;

2° de persoonsgegevens van de eindgebruiker;

3° de datum en het tijdstip waarop de e-mail- of internettelefonieaccount is gecreëerd;

4° het IP-adres en de bronpoort die gediend hebben voor de creatie van de e-mail- of internettelefonieaccount;

5° de gegevens betreffende betalingswijze, identificatie van het betaalmiddel en tijdstip van de betaling voor het abonnement of het gebruik van de dienst.

§ 2. Wat de verkeers- en locatiegegevens betreft, bewaren de aanbieders van een openbare e-maildienst via internet, de aanbieders van een openbare internettelefoniedienst en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° de eindgebruikersidentificatie met betrekking tot de e-mail- of internettelefonieaccount, alsook het nummer of de identificatiecode van de beoogde ontvanger van de communicatie;

2° het telefoonnummer toegewezen aan elke communicatie die het openbare telefoonnetwerk binnenkomt in het kader van een internettelefoniedienst;

3° *a)* het IP-adres en de bronpoort die worden gebruikt door de eindgebruiker;

b) het IP-adres en de bronpoort die worden gebruikt door de bestemmeling;

4° de datum en het tijdstip van de log-in en log-off van een sessie van een e-maildienst via internet of internettelefoniedienst;

5° de datum en het tijdstip van een verbinding die tot stand wordt gebracht met behulp van de internet-telefonieaccount;

6° de technische karakteristieken van de gebruikte dienst.

§ 3. De in paragraaf 1 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, eerste lid, van de wet.

De in paragraaf 2 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, tweede lid, van de wet ».

B.16.6. Dat koninklijk besluit bepaalt evenwel geen minimale of maximale bewaartermijn van de krachtens artikel 127 van de wet van 13 juni 2005 verwerkte identificatiegegevens. Die termijn was immers verankerd in het bij het arrest nr. 57/2021 vernietigde artikel 126, § 3, van de wet van 13 juni 2005, dat bepaalde :

« De gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen, met uitzondering van de gegevens waarin het tweede en derde lid specifiek voorzien, worden gedurende twaalf maanden bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst.

De gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, worden bewaard gedurende twaalf maanden, vanaf de datum van de communicatie.

De communicatiegegevens, met uitzondering van de inhoud, met inbegrip van hun herkomst en hun bestemming, worden gedurende twaalf maanden bewaard vanaf de datum van de communicatie.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de te bewaren gegevens per type van categorie bedoeld in het eerste tot derde lid alsook de vereisten waaraan deze gegevens moeten beantwoorden ».

In afwachting van de inwerkingtreding van een nieuwe versie van artikel 126 van de wet van 13 juni 2005 wordt de eindgebruiker van een vooraf betaalde belkaart evenwel niet onderworpen aan een risico op onbeperkte bewaring van zijn identificatiegegevens. De thans toepasselijke versie van die bepaling vermeldt immers een uiterste bewaartermijn van 36 maanden.

Daarnaast geniet die eindgebruiker de bescherming van de AVG, die door de bevoegde gegevensverwerker dient te worden geëerbiedigd naast - en desnoods met voorrang op - de toepasselijke bepalingen van nationaal recht. Krachtens het in artikel 5, *e)*, van de AVG neergelegde beginsel van de opslagbeperking dient de gegevensverwerker de persoonsgegevens te bewaren « in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is ».

Gelet op die bepalingen kan worden aanvaard dat, in afwachting van de inwerkingtreding van een nieuw wetgevend kader inzake dataretentie, de toepasselijke wetgeving tijdelijk niet in een specifieke bewaartermijn voorziet. Het staat in tussentijd aan de bevoegde bestuurlijke autoriteiten en rechtscolleges om op grond van die bepalingen te waarborgen dat de identificatiegegevens van de eindgebruikers van vooraf betaalde belkaarten niet langer worden bewaard dan noodzakelijk is in het licht van de met de bestreden identificatieplicht nagestreefde doelstellingen.

B.16.7. Die doelstellingen worden op limitatieve wijze opgesomd in artikel 127, § 1, van de wet van 13 juni 2005. Het gaat om de goede werking van de nooddiensten, het strafrechtelijk onderzoek en de werking van de inlichtingen- en veiligheidsdiensten. Die tweede en derde doelstelling komen overeen met de redenen waarvoor het Hof van Justitie de bewaring van identificatiegegevens toestaat (HvJ, grote kamer, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, punten 152 tot 159). De goede werking van de nooddiensten houdt dan weer verband met de positieve verplichtingen die op de overheden rusten in het kader van de rechten die slachtoffers van misdrijven en ongevallen putten uit de artikelen 2, 3, 5 en 8 van het Europees Verdrag voor de rechten van de mens.

B.16.8.1. De wetgeving op die diensten vermeldt bovendien op limitatieve wijze welke autoriteiten toegang hebben tot de bewaarde identificatiegegevens en aan welke materiële en procedurele voorwaarden zij daartoe dienen te voldoen.

B.16.8.2. De toegang tot die gegevens in het kader van een opsporingsonderzoek en strafrechtelijk onderzoek wordt geregeld door de artikelen 46*bis*, 88*bis* en 90*ter* tot 90*decies* van het Wetboek van strafvordering.

Artikel 46*bis* van het Wetboek van strafvordering bepaalt :

« § 1. Bij het opsporen van de misdaden en wanbedrijven kan de procureur des Konings bij een met redenen omklede en schriftelijke beslissing overgaan of doen overgaan op basis van ieder gegeven in zijn bezit of door middel van een toegang tot de klantenbestanden van de actoren bedoeld in het tweede lid, eerste en tweede streepje, tot :

1° de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in het tweede lid, tweede streepje, of van het gebruikte elektronische communicatiemiddel;

2° de identificatie van de diensten bedoeld in het tweede lid, tweede streepje, waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.

Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van :

- de operator van een elektronisch communicatienetwerk, en

- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

De motivering weerspiegelt de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

In geval van uiterst dringende noodzakelijkheid kan de procureur des Konings de maatregel mondeling bevelen. De beslissing wordt zo spoedig mogelijk schriftelijk bevestigd.

Voor strafbare feiten die geen correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, kan de procureur des Konings de in het eerste lid bedoelde gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan zijn beslissing.

§ 2. De actoren bedoeld in § 1, tweede lid, eerste en tweede streepje, van wie gevorderd wordt de in paragraaf 1 bedoelde gegevens mee te delen, verstrekken de procureur des Konings of de officier van gerechtelijke politie de gegevens in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, volgens de nadere regels vastgesteld door de Koning, op het voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie.

De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en op voorstel van de Minister van Justitie en van de minister die bevoegd is voor Telecommunicatie, de technische voorwaarden voor de toegang tot de in § 1 bedoelde gegevens, die beschikbaar zijn voor de procureur des Konings en voor de in dezelfde paragraaf aangewezen politiedienst.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro ».

Artikel 88*bis* van het Wetboek van strafvordering bepaalt :

« § 1. Wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben en de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij :

1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;

2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren.

Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van :

- de operator van een elektronisch communicatienetwerk; en

- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

In de gevallen bedoeld in het eerste lid wordt voor ieder elektronisch communicatiemiddel waarvan de verkeersgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de elektronische communicatie vastgesteld en opgenomen in een proces-verbaal.

De onderzoeksrechter doet in een met redenen omkleed bevelschrift opgave van de feitelijke omstandigheden van de zaak die de maatregel rechtvaardigen, van de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

Hij vermeldt ook de duur van de maatregel voor de toekomst, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, onverminderd een hernieuwing en, in voorkomend geval, de periode in het verleden waarover de vordering zich uitstrekt overeenkomstig paragraaf 2.

In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in artikel 90*ter*, §§ 2, 3 en 4, bedoelde strafbare feiten. In dat geval moet de maatregel binnen vierentwintig uur worden bevestigd door de onderzoeksrechter.

Indien het echter het in artikel 137, 347*bis*, 434 of 470 van het Strafwetboek bedoelde strafbare feit betreft, met uitzondering van het in artikel 137, § 3, 6°, van hetzelfde Wetboek bedoelde strafbare feit, kan de procureur des Konings de maatregel bevelen zolang de heterdaadsituatie duurt, zonder dat een bevestiging door de onderzoeksrechter nodig is.

Indien het het in artikel 137 van het Strafwetboek bedoelde strafbare feit betreft, met uitzondering van het in artikel 137, § 3, 6°, van hetzelfde Wetboek bedoelde strafbare feit, kan de procureur des Konings bovendien de maatregel bevelen binnen de tweeënzeventig uur na de ontdekking van dit strafbare feit, zonder dat een bevestiging door de onderzoeksrechter nodig is.

De procureur des Konings kan evenwel de maatregel bevelen indien de klager erom verzoekt, wanneer deze maatregel onontbeerlijk lijkt voor het vaststellen van een strafbaar feit bedoeld in artikel 145, § 3 en § 3*bis* van de wet van 13 juni 2005 betreffende de elektronische communicatie.

In spoedeisende gevallen kan de maatregel mondeling worden bevolen. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het vierde en vijfde lid.

§ 2. Wat betreft de toepassing van de maatregel bedoeld in paragraaf 1, eerste lid, op de verkeers- of lokalisatiegegevens die worden bewaard krachtens artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing :

- voor een strafbaar feit bedoeld in boek II, titel I*ter*, van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan zijn bevelschrift;

- voor een ander strafbaar feit bedoeld in artikel 90*ter*, §§ 2 tot 4, dat niet bedoeld is in het eerste gedachtestreepje, of een strafbaar feit dat gepleegd is in het kader van een criminele organisatie als bedoeld in artikel 324*bis* van het Strafwetboek, of een strafbaar feit dat een hoofdgevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kan hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;

- voor andere strafbare feiten kan de onderzoeksrechter de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift.

§ 3. De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.

De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte werd gebracht. Diezelfden zullen door de onderzoeksrechter in kennis worden gesteld van hetgeen volgens hem onder het beroepsgeheim valt. Deze gegevens worden niet opgenomen in het proces-verbaal. Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 4. De actoren bedoeld in § 1, tweede lid, delen de gegevens waarom verzocht werd mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, volgens de nadere regels vastgesteld door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die zijn technische medewerking aan de vorderingen bedoeld in dit artikel weigert of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, medewerking waarvan de nadere regels vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro ».

Artikel 90*ter*, § 1, van het Wetboek van strafvordering bepaalt :

« § 1. De onderzoeksrechter kan, onverminderd de toepassing van artikelen 39*bis*, 87, 88, 89*bis* en 90, met een heimelijk oogmerk, niet voor het publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan met technische hulpmiddelen onderscheppen, er kennis van nemen, doorzoeken en opnemen of de zoeking in een informaticasysteem of een deel ervan uitbreiden.

Deze maatregel kan enkel worden bevolen in uitzonderlijke gevallen, wanneer het onderzoek zulks vereist, indien er ernstige aanwijzingen bestaan dat het een strafbaar feit betreft bedoeld in paragraaf 2, en indien de overige middelen van onderzoek niet volstaan om de waarheid aan de dag te brengen.

Teneinde deze maatregel mogelijk te maken, kan de onderzoeksrechter bevelen om, te allen tijde, ook buiten medeweten of zonder de toestemming van hetzij de bewoner, hetzij de eigenaar of zijn rechthebbende, hetzij de gebruiker :

- in een woning, in een private plaats of in een informaticasysteem binnen te dringen;

- elke beveiliging van de betrokken informaticasystemen tijdelijk op te heffen, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden;

- technische middelen in de betrokken informaticasystemen aan te brengen teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen.

De maatregel bedoeld in deze paragraaf kan alleen worden bevolen om de gegevens op te sporen die kunnen dienen om de waarheid aan de dag te brengen. Hij kan alleen worden bevolen ten aanzien van personen die op grond van precieze aanwijzingen ervan verdacht worden het strafbare feit te hebben gepleegd, ten aanzien van de communicatiemiddelen of informaticasystemen die geregeld worden gebruikt door een persoon op wie een verdenking rust of ten aanzien van de plaatsen waar deze vermoed wordt te vertoeven. De maatregel kan eveneens worden bevolen ten aanzien van personen van wie op grond van precieze feiten vermoed wordt dat zij geregeld in verbinding staan met een persoon op wie een verdenking rust ».

B.16.8.3. De toegang tot die gegevens in het kader van een onderzoek door de inlichtingen- en veiligheidsdiensten wordt geregeld door artikel 16/2, § 1, van de wet van 30 november 1998, dat bepaalt :

« De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst om over te gaan tot :

1° het identificeren van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel;

2° het identificeren van de elektronische communicatiediensten en -middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt.

De vordering gebeurt schriftelijk door het diensthoofd of zijn gedelegeerde. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze gegevens mondeling vorderen. Deze mondelinge vordering wordt binnen vierentwintig uur bevestigd door een schriftelijke vordering.

Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die wordt gevorderd, verstrekt aan het diensthoofd of zijn gedelegeerde de gegevens waar om werd verzocht binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op het voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de elektronische communicatie.

Het diensthoofd of zijn gedelegeerde kan, mits naleving van de principes van proportionaliteit en subsidiariteit en mits de registratie van de raadpleging, de bedoelde gegevens ook verkrijgen met behulp van toegang tot de klantenbestanden van de operator of van de dienstenverstrekker. De Koning bepaalt, op voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de elektronische communicatie, de technische voorwaarden waaronder deze toegang mogelijk is ».

B.16.8.4. De toegang tot die gegevens door de nooddiensten wordt geregeld door artikel 107, § 2, van de wet van 13 juni 2005, dat bepaalt :

« De operatoren betrokken bij een noodoproep naar een nooddienst die ter plaatse hulp biedt, indien nodig met onderlinge coördinatie, leveren gratis aan de beheerscentrales van deze nooddienst de identificatiegegevens van de oproeper zodra deze de oproep ontvangen.

Deze verplichting is eveneens van toepassing wanneer de beheerscentrales van de nooddiensten die ter plaatse hulp bieden geëxploiteerd worden door een organisatie die vanwege de overheid met deze opdracht is belast.

De investerings- en exploitatiekosten met betrekking tot de databanken met de identificatiegegevens van de oproeper en met betrekking tot de toegangslijnen die door de nooddiensten gebruikt worden om deze databanken te raadplegen, komen ten laste van de operatoren.

Indien een operator zijn eigen commerciële diensten aanbiedt voor het aanleveren van locatiegegevens aan abonnees, moeten de nauwkeurigheid van de locatiegegevens die deel uitmaken van de identificatie van de oproeper bij een noodoproep en welke overeenkomstig deze paragraaf geleverd dienen te worden aan de nooddiensten die ter plaatse hulp bieden, alsook de snelheid waarmee deze overgezonden worden aan de betrokken nooddienst, ten minste gelijk zijn aan de beste kwaliteit die door die operator commercieel wordt aangeboden. Het Instituut kan in overleg met de betrokken nooddiensten de criteria voor de nauwkeurigheid en betrouwbaarheid van de verstrekte locatiegegevens over de oproeper vaststellen.

De identificatie van de oproeper kan, door de nooddiensten die ter plaatse hulp bieden of de organisatie die vanwege de overheid is belast met de exploitatie van de beheerscentrales van deze nooddiensten en aan de hand van administratieve en technische maatregelen die worden goedgekeurd door de minister, op advies van het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer, worden aangewend om kwaadwillige oproepen of het misbruik van de noodnummers te bestrijden. Deze maatregelen mogen echter niet tot gevolg hebben dat de toegang tot het noodnummer van de desbetreffende nooddienst vanaf een welbepaalde aansluiting onmogelijk is tijdens een ononderbroken periode die langer is dan vierentwintig uur.

De beheerscentrales van de nooddiensten die op afstand hulp bieden krijgen, teneinde noodoproepen te kunnen behandelen en kwaadwillige oproepen te kunnen bestrijden, van de betrokken operatoren gratis de voor de operatoren in hun netwerk beschikbare identificatie van de oproepende lijn, zelfs indien de gebruiker stappen ondernomen heeft om de verzending van de identificatie te verhinderen. Het formaat van de identificatie van de oproepende lijn dat geleverd wordt, dient in overeenstemming te zijn met de toepasselijke ETSI-standaarden en wordt gedefinieerd door het Instituut in overleg met de nooddiensten en de operatoren.

De identificatie van de oproepende lijn kan door de nooddiensten die op afstand hulp bieden en aan de hand van administratieve en technische maatregelen die worden goedgekeurd door de minister, op advies van het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer, worden aangewend om kwaadwillige oproepen te bestrijden. Deze maatregelen mogen echter niet tot gevolg hebben dat de toegang tot het noodnummer van de desbetreffende nooddienst vanaf een welbepaalde aansluiting onmogelijk is tijdens een ononderbroken periode die langer is dan vierentwintig uur ».

B.16.8.5. Die bepalingen regelen op duidelijke en nauwkeurige wijze de materiële en procedurele voorwaarden waaronder die autoriteiten toegang kunnen hebben tot de krachtens artikel 127 van de wet van 13 juni 2005 verwerkte identificatiegegevens.

Wanneer zij zich toegang tot die gegevens verschaffen, dienen die autoriteiten niet alleen de in B.16.8.2 tot B.16.8.4 vermelde regels na te leven, maar ook de grondrechten van de eindgebruiker te eerbiedigen, zoals die onder meer zijn gewaarborgd door de AVG, de artikelen 6 en 8 van het Europees Verdrag voor de rechten van de mens en de artikelen 7, 8 en 47 van het Handvest.

B.16.8.6. In dat verband verwijzen de verzoekende partijen naar het arrest van de grote kamer van het Hof van Justitie van 2 maart 2021 in zake *Prokuratuur* (C-746/18, punten 50 tot 56), waarin het Hof van Justitie volgens hen eist dat een onafhankelijke bestuurlijke autoriteit of een rechter elk verzoek tot toegang voorafgaandelijk toetst aan de toepasselijke nationale regels en grondrechten en waarin het volgens hen preciseert dat het openbaar ministerie, dat de onderzoeksprocedure leidt en in voorkomend geval optreedt als aanklager, niet over de vereiste onafhankelijkheid beschikt om die toetsing te kunnen doorvoeren.

Dat arrest had evenwel betrekking op een verzoek van het openbaar ministerie om toegang te krijgen tot verkeers- en locatiegegevens. Zoals uiteengezet in B.14.3, vereisen het Hof van Justitie en het Europees Hof voor de Rechten van de Mens daarentegen geen voorafgaande rechterlijke of bestuurlijke toetsing van een verzoek om toegang tot identificatiegegevens. Bijgevolg verzet het recht op eerbiediging van het privéleven zich niet tegen een verzoek tot toegang tot dergelijke gegevens dat uitgaat van het openbaar ministerie.

B.16.8.7. Wel dient het verzoek om toegang tot de krachtens artikel 127 van de wet van 13 juni 2005 verwerkte identificatiegegevens steeds *in concreto* te worden gemotiveerd door het verband aan te tonen tussen die gegevens en de objectieve elementen die de initiële concrete verdenking van de betrokken eindgebruiker voor een specifiek misdrijf ondersteunen. Tevens dient te worden gemotiveerd dat er niet meer gegevens worden opgevraagd dan strikt noodzakelijk is in het licht van het lopende onderzoek. Een dergelijke motivering mag geen gebruik maken van standaardformuleringen of stijlformules.

B.16.9.1. De wet van 13 juni 2005 en de koninklijke besluiten van 19 september 2013 en 26 november 2016 bevatten waarborgen tegen misbruik in het kader van de verzameling, verwerking en bewaring van de identificatiegegevens.

Artikel 127, § 1, van de wet van 13 juni 2005 bepaalt dat het verkoopkanaal van elektronische-communicatiediensten de verzamelde identificatiegegevens en identificatiedocumenten naar de operator doorstuurt, zonder zelf kopieën te bewaren. Indien een rechtstreekse invoer van die gegevens in het computersysteem niet mogelijk is, kan het verkoopkanaal een tijdelijke kopie van het identificatiedocument maken, die het uiterlijk op het ogenblik van de activering van de vooraf betaalde belkaart vernietigt.

Krachtens artikel 11, § 1, van het koninklijk besluit van 27 november 2016 dient de betrokken onderneming systematisch te verifiëren of een voorgelegde identiteitskaart niet werd gestolen of niet het voorwerp heeft uitgemaakt van fraude. Krachtens artikel 12, derde lid, van hetzelfde koninklijk besluit dient de betrokken onderneming of de leverancier van een identificatiedienst de kopie van de foto op de elektronische identiteitskaart te vernietigen uiterlijk vóór de activering van de vooraf betaalde belkaart.

Krachtens artikel 8 van het koninklijk besluit van 19 september 2013 dient elke aanbieder onder de leden van de Coördinatiecel Justitie een aangestelde voor de bescherming van de persoonsgegevens aan te wijzen, die voor de bescherming van de persoonsgegevens in volledige onafhankelijkheid ten opzichte van die aanbieder handelt en toegang heeft tot alle relevante gegevens en lokalen van die aanbieder. Hij dient erop toe te zien dat alle verwerkingen de in artikel 126 van de wet van 13 juni 2005 vermelde doelstellingen nastreven, dat enkel de krachtens die bepaling en het koninklijk besluit van 19 september 2013 gemachtigde personen toegang hebben tot de gegevens, en dat alle maatregelen ter bescherming van de in artikel 126 van de wet van 13 juni 2005 beschreven gegevens in acht worden genomen.

B.16.9.2. Op het niveau van de toegang tot de bewaarde gegevens, bepaalt artikel 9 van het koninklijk besluit van 19 september 2013 dat elke aanbieder jaarlijks vóór 1 maart aan het Belgisch Instituut voor postdiensten en telecommunicatie meedeelt hoe vaak in het afgelopen kalenderjaar gegevens zijn verstrekt aan de bevoegde autoriteiten, hoeveel tijd er is verstreken tussen de verwerking en het opvragen van de gegevens en in welke gevallen de verzoeken om gegevens niet konden worden ingewilligd. Dat Instituut bezorgt die inlichtingen jaarlijks aan de minister van Justitie.

Krachtens artikel 90*decies* van het Wetboek van strafvordering dient de minister van Justitie bovendien jaarlijks verslag uit te brengen aan het Parlement over de toepassing van onder meer de artikelen 46*bis*, 88*bis* en 90*ter* tot 90*novies* van hetzelfde Wetboek. Die kennisgeving betreft het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in die artikelen, de duur van die maatregelen, het aantal betrokken personen en de behaalde resultaten.

Krachtens artikel 21 van de wet van 30 november 1998 worden de persoonsgegevens die in het kader van die wet worden verwerkt, door de inlichtingen- en veiligheidsdiensten bewaard voor een duur die niet langer mag zijn dan die welke noodzakelijk is voor de doeleinden waarvoor ze opgeslagen worden.

Het door het Hof bij zijn arrest nr. 57/2021 vernietigde artikel 126, §§ 4 tot 6, van de wet van 13 juni 2005, bepaalde nog verdere waarborgen tegen misbruik :

« § 4. Wat betreft de bewaring van de gegevens bedoeld in paragraaf 3, dienen de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid :

1° te garanderen dat de bewaarde gegevens dezelfde kwaliteit hebben en onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;

2° ervoor te zorgen dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies of wijziging per ongeluk, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking;

3° te garanderen dat de toegang tot de bewaarde gegevens om te antwoorden op de verzoeken van de autoriteiten bedoeld in paragraaf 2, enkel gebeurt door een of meer leden van de Coördinatiecel bedoeld in artikel 126/1, § 1;

4° de gegevens op het grondgebied van de Europese Unie te bewaren;

5° te zorgen voor maatregelen van technologische beveiliging die de bewaarde gegevens, vanaf hun registratie, onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er toegang toe te hebben;

6° ervoor te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt zoals vastgelegd in paragraaf 3, worden verwijderd van elke drager, onverminderd de artikelen 122 en 123;

7° ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord voor elk verzoek om deze gegevens te verkrijgen vanwege een autoriteit bedoeld in paragraaf 2.

De in het eerste lid, 7°, bedoelde opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer mogen dat logboek raadplegen of een kopie van een deel of van het geheel van dat logboek eisen. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer sluiten een protocol tot samenwerking voor de raadpleging van en het toezicht op dat logboek.

§ 5. De minister en de minister van Justitie zorgen ervoor dat statistieken inzake de bewaring van de gegevens die worden gegenereerd of verwerkt in het kader van de verstrekking van openbaar toegankelijke communicatienetwerken en -diensten jaarlijks worden bezorgd aan de Kamer van volksvertegenwoordigers.

Die statistieken omvatten met name :

1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens zijn verstrekt aan de bevoegde autoriteiten;

2° de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;

3° de gevallen waarin verzoeken om gegevens niet konden worden ingewilligd.

Die statistieken mogen geen persoonsgegevens omvatten.

De gegevens die betrekking hebben op de toepassing van paragraaf 2, 1°, worden tevens bijgevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90*decies* van het Wetboek van strafvordering moet uitbrengen aan het Parlement.

De Koning bepaalt, op voorstel van de minister van Justitie en de minister en op advies van het Instituut, de statistieken die de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, jaarlijks bezorgen aan het Instituut en die welke het Instituut bezorgt aan de minister en aan de minister van Justitie.

§ 6. Onverminderd het verslag bedoeld in paragraaf 5, vierde lid, brengen de minister en de minister van Justitie, twee jaar na de inwerkingtreding van het in paragraaf 3, vierde lid, bedoelde koninklijk besluit een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel, teneinde na te gaan of het nodig is bepalingen aan te passen, inzonderheid wat betreft de te bewaren gegevens en de bewaringstermijn ».

Het staat aan de wetgever om, wanneer hij een nieuw wetgevend kader inzake dataretentie schept dat voldoet aan de in het arrest nr. 57/2021 vermelde criteria, waarborgen tegen misbruik daarin opnieuw op te nemen. In afwachting daarvan mag - gelet op de andere vermelde waarborgen tegen misbruik - de afwezigheid van een dergelijke bepaling, die slechts betrekking heeft op de toegang tot de bewaarde persoonsgegevens, niet leiden tot de vernietiging van de bestreden wet, die immers slechts handelt over de initiële verzameling, verwerking en bewaring van de identificatiegegevens van gebruikers van een vooraf betaalde belkaart.

B.16.10. Artikel 127 van de wet van 13 juni 2005 bepaalt geen specifiek rechterlijk toezicht op de verwerking van de krachtens artikel 127 van de wet van 13 juni 2005 verwerkte identificatiegegevens. Zoals in B.14.3 werd uiteengezet, volstaan inzake de verwerking van en de toegang tot loutere identificatiegegevens evenwel de gemeenrechtelijke rechtsmiddelen (EHRM, 30 januari 2020, *Breyer t. Duitsland*, § 106).

In het kader van de strafprocedure beschikt de beklaagde in dat verband over het recht om voor de onderzoeksgerechten of voor de vonnisrechter de nietigheid van een onderzoekshandeling aan te voeren die zijn recht op eerbiediging van het privéleven of zijn recht op een eerlijk proces schendt.

In het kader van de werking van de inlichtingen- en veiligheidsdiensten beschikt de betrokkene krachtens artikel 79 van de wet van 30 juli 2018 « betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens » over het recht om aan het Vast Comité I te vragen zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen en de naleving van de toepasselijke bepalingen te verifiëren.

Tevens beschikt elke eindgebruiker van een vooraf betaalde belkaart wiens identificatiegegevens in strijd met artikel 127 van de wet van 13 juni 2005 en het koninklijk besluit van 27 november 2016 zijn verwerkt, over een gemeenrechtelijke aansprakelijkheidsvordering tegen de persoon die die wetsbepaling heeft overtreden.

Tot slot kan de betrokkene krachtens artikel 58 van de wet van 3 december 2017 « tot oprichting van de Gegevensbeschermingsautoriteit » kosteloos een klacht indienen bij de Gegevensbeschermingsautoriteit in geval van een onrechtmatige verwerking van zijn persoonsgegevens.

B.16.11.1. De drie legitieme doelstellingen die de wetgever met artikel 127 van de wet van 13 juni 2005 nastreeft, te weten de goede werking van de nooddiensten, het opsporen, vervolgen en bestraffen van misdrijven en de informatieverwerving door de inlichtingen- en veiligheidsdiensten, houden alle verband met de positieve verplichtingen die op de overheid rusten met betrekking tot het recht op leven, het verbod op onmenselijke en vernederende behandeling en het recht op vrijheid en veiligheid van de ganse bevolking.

B.16.11.2. Een maatregel die voorziet in de identificeerbaarheid van alle eindgebruikers van een vooraf betaalde belkaart is pertinent om die doelstellingen te bereiken.

De mogelijkheid om een vooraf betaalde belkaart te vervreemden en de mogelijkheid dat zij gestolen wordt, volstaan niet om daarover anders te besluiten. Artikel 127, § 1, derde lid, van de wet van 13 juni 2005 bepaalt daarom overigens dat de geïdentificeerde persoon wordt geacht zelf de elektronische-communicatiedienst te gebruiken. Die bepaling beoogt hem tot voorzichtigheid aan te zetten inzake het gebruik van zijn vooraf betaalde belkaart door derden. Artikel 5 van het koninklijk besluit van 27 november 2016 beperkt bovendien de mogelijkheid om een vooraf betaalde belkaart aan derden over te dragen : behoudens de hypothese waarin de belkaart wordt overgedragen aan een nauw familielid (artikel 5, 1° tot 3°), is een overdracht slechts mogelijk indien die derde zich vooraf identificeert bij de betrokken onderneming (artikel 5, 4°), indien een rechtspersoon die een belkaart geeft aan een natuurlijke persoon die voor hem diensten verricht, daar een geactualiseerde lijst van bijhoudt (artikel 5, 5°), of indien de belkaart wordt gekocht voor rekening van de inlichtingen- en veiligheidsdiensten, de politiediensten of bepaalde bij koninklijk besluit aangeduide overheden (artikel 5, 6°). Artikel 6 van hetzelfde koninklijk besluit verplicht de eindgebruiker om binnen 24 uur na het verlies of de diefstal van de belkaart de betrokken onderneming daarvan op de hoogte te brengen.

Ook het bestaan van andere communicatietechnieken verhindert de wetgever niet om de anonimiteit van de vooraf betaalde belkaarten af te schaffen indien hij vaststelt dat met name die belkaarten worden gebruikt in terroristische en criminele milieus en dat die anonimiteit een onoverkomelijk probleem vormt voor de gerechtelijke overheden en voor de inlichtingen- en veiligheidsdiensten. Indien de bestreden bepaling als gevolg heeft dat terroristische en criminele organisaties overstappen naar meer geavanceerde technieken, toont dat overigens veeleer de pertinentie van de bestreden maatregel aan. Het staat dan aan de wetgever om met het oog op dezelfde doelstellingen ook het gebruik van die technieken te reguleren.

B.16.11.3. Gelet op de in B.16.1 tot B.16.9.3 vermelde waarborgen is de identificeerbaarheid van de eindgebruiker van een vooraf betaalde belkaart, die als een maatregel met een geringe privacygevoeligheid dient te worden aangemerkt, tevens evenredig in het licht van die doelstellingen. Het feit dat die maatregel slaat op alle eindgebruikers van vooraf betaalde belkaarten, ook indien zij niet kunnen worden verdacht van enig crimineel gedrag, doet daaraan geen afbreuk, aangezien een maatregel van identificeerbaarheid slechts kan werken voor zover eenieder kan worden geïdentificeerd zodra dat nodig is.

B.16.11.4. Tot slot konden de gebruikers van vooraf betaalde belkaarten niet onwetend zijn over het feit dat de anonimiteit van die belkaarten ooit zou worden afgeschaft. Zoals in B.2.1 tot B.2.7 werd uiteengezet, was die anonimiteit immers steeds opgevat als een tijdelijke uitzondering op de regel dat alle eindgebruikers van elektronische-communicatienetwerken identificeerbaar moeten zijn.

B.16.12. Onder voorbehoud van de in B.8.7.3, B.16.6, B.16.8.5 en B.16.8.7 vermelde interpretaties is het eerste onderdeel van het tweede middel niet gegrond.

Wat betreft het tweede onderdeel van het tweede middel

B.17. In het tweede onderdeel van het tweede middel voeren de verzoekende partijen aan dat de bestreden wet de vrijheid van vestiging en met het vrij verrichten van diensten schendt.

B.18. Elke nationale maatregel die tot gevolg kan hebben dat het vrij verrichten van diensten door ondernemingen uit een andere lidstaat van de Europese Unie wordt belemmerd of minder aantrekkelijk wordt, is een beperking van het vrij verrichten van diensten. Voorts kent artikel 56 van het Verdrag betreffende de werking van de Europese Unie niet alleen rechten toe aan de dienstverrichter zelf, maar ook aan de ontvanger van de diensten.

Een dergelijke beperking kan evenwel haar rechtvaardiging vinden « in dwingende redenen van algemeen belang indien zij geschikt [is] om de verwezenlijking van het nagestreefde doel te verzekeren en niet verder [gaat] dan noodzakelijk is om dit doel te bereiken, wat inhoudt dat er geen minder beperkende maatregelen zijn die even doeltreffend zouden zijn om dat doel te bereiken » (HvJ, 11 februari 2021, C-407/19 en C-471/19, *Katoen Natie Bulk Terminals NV e.a.*, punten 59 tot 61).

B.19.1. Zonder dat het nodig is te onderzoeken of de bestreden wet de vrijheid van vestiging of het vrij verrichten van diensten beperkt, volstaat de vaststelling dat zij wordt gerechtvaardigd door dwingende redenen van algemeen belang, namelijk de goede werking van de nooddiensten, de effectieve opsporing, vervolging en bestraffing van strafbare feiten en het voorkomen van terroristische activiteiten door te verzekeren dat de inlichtingen- en veiligheidsdiensten potentiële dreigingen kunnen koppelen aan de identiteit van personen wier communicatie zij onderscheppen.

B.19.2. Zoals in B.16.11.2 werd uiteengezet, is de bestreden wet geschikt om die doelstellingen te bereiken. Tevens gaat zij niet verder dan noodzakelijk om ze te bereiken. Een maatregel die beoogt te verzekeren dat de eindgebruikers van een Belgisch elektronische-communicatienetwerk identificeerbaar zijn, kan immers slechts nut hebben indien hij zonder uitzondering van toepassing is op alle eindgebruikers ervan, ongeacht of zij met een abonnement of met een vooraf betaalde belkaart bellen, ongeacht of die belkaart reeds was aangekocht vóór de inwerkingtreding van de bestreden wet, en ongeacht of het gaat om een belkaart die wordt geleverd door een in België of in een andere lidstaat van de Europese Unie gevestigde onderneming.

De uitsluiting van vooraf betaalde belkaarten die worden geleverd door in een andere lidstaat gevestigde ondernemingen uit het toepassingsgebied van artikel 127 van de wet van 13 juni 2005 zou de identificeerbaarheid in de praktijk onmogelijk maken, aangezien met name personen met kwaadwillige intenties zich er eenvoudig aan zouden kunnen onttrekken door een vooraf betaalde belkaart van een in een andere lidstaat gevestigde onderneming aan te schaffen.

B.19.3. Het tweede onderdeel van het tweede middel is niet gegrond.

Wat betreft het derde onderdeel van het tweede middel

B.20. In het derde onderdeel van het tweede middel voeren de verzoekende partijen aan dat de bestreden wet de vrijheid van meningsuiting schendt, aangezien de identificeerbaarheid van eindgebruikers van een vooraf betaalde belkaart hen zou ontmoedigen om politici en journalisten te informeren en aldus de vrijheid om inlichtingen en denkbeelden te ontvangen en het journalistieke bronnengeheim op onevenredige wijze zou beperken.

B.21.1. De vrijheid van meningsuiting is een van de pijlers van een democratische samenleving. Zij geldt niet alleen voor de « informatie » of de « ideeën » die gunstig worden onthaald of die als onschuldig of onverschillig worden beschouwd, maar ook voor die welke de Staat of een of andere groep van de bevolking « schokken, verontrusten of kwetsen ». Zo willen het het pluralisme, de verdraagzaamheid en de geest van openheid, zonder welke er geen democratische samenleving kan bestaan (EHRM, 7 december 1976, *Handyside t. Verenigd Koninkrijk*, § 49; 23 september 1998, *Lehideux en Isorni t. Frankrijk*, § 55; 28 september 1999, *Öztürk t. Turkije*, § 64; grote kamer, 13 juli 2012, *Mouvement raëlien suisse t. Zwitserland*, § 48).

Niettemin brengt de uitoefening van de vrijheid van meningsuiting, zoals blijkt uit de bewoordingen van artikel 10, lid 2, van het Europees Verdrag voor de rechten van de mens, bepaalde plichten en verantwoordelijkheden met zich mee (EHRM, 4 december 2003, *Gündüz t. Turkije*, § 37), onder meer de principiële plicht bepaalde grenzen « die meer bepaald de bescherming van de goede naam en de rechten van anderen nastreven » niet te overschrijden (EHRM, 24 februari 1997, *De Haes en Gijsels t. België*, § 37; 21 januari 1999, *Fressoz en Roire t. Frankrijk*, § 45; 15 juli 2003, *Ernst e.a. t. België*, § 92). De vrijheid van meningsuiting kan, krachtens artikel 10, lid 2, van het Europees Verdrag voor de rechten van de mens, onder bepaalde voorwaarden worden onderworpen aan formaliteiten, voorwaarden, beperkingen of sancties, met het oog op, onder meer, de bescherming van de goede naam of de rechten van anderen. De uitzonderingen waarmee zij gepaard gaat, dienen echter « eng te worden geïnterpreteerd, en de noodzaak om haar te beperken moet op overtuigende wijze worden aangetoond » (EHRM, grote kamer, 20 oktober 2015, *Pentikäinen t. Finland*, § 87).

Artikel 19 van de Grondwet verbiedt dat de vrijheid van meningsuiting aan preventieve beperkingen wordt onderworpen, maar niet dat misdrijven die ter gelegenheid van het gebruikmaken van die vrijheid worden gepleegd, worden bestraft.

B.21.2. Het recht op geheimhouding van de journalistieke bronnen dient te worden gewaarborgd, niet zozeer ter bescherming van de belangen van de journalisten als beroepsgroep, maar wel om het de pers mogelijk te maken haar rol van « waakhond » te spelen en het publiek in te lichten over kwesties van algemeen belang. Om die reden maakt dat recht deel uit van de vrijheid van meningsuiting en de persvrijheid.

B.21.3. Volgens het Hof van Justitie kan « de doorzending van verkeers- en locatiegegevens aan overheidsinstanties voor veiligheidsdoeleinden [...] de gebruikers [...] ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen. Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (*Pb.* 2019, L-305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde gegevens talrijk en gevarieerd zijn » (HvJ, grote kamer, 6 oktober 2020, C-623/17, *Privacy International*, punt 72; zie in dezelfde zin HvJ, grote kamer, 8 april 2014, C-293/12 en C-594/12, *Digital Rights Ireland e.a.*, punt 28; 21 december 2016, C-203/15 en C-698/15, *Tele2 Sverige e.a.*, punt 101; 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, punt 118).

B.22. Artikel 127 van de wet van 13 juni 2005 heeft slechts betrekking op de bewaring en verwerking van de identificatiegegevens bedoeld in artikel 12 van het koninklijk besluit van 27 november 2016. Dergelijke gegevens geven op zich geen inzicht in de persoonlijke standpunten van de geïdentificeerde persoon. Ook de verkeers- en locatiegegevens waaraan zij zouden kunnen worden gekoppeld, maken op zich geen meningsuiting uit.

Pas wanneer die gegevens tevens zouden worden gekoppeld aan de inhoud van een gevoerde communicatie, en de analyse daarvan aanleiding geeft tot verdere maatregelen, zoals het voeren van een onderzoek door de inlichtingen- en veiligheidsdiensten of het opstarten van een strafrechtelijk onderzoek, kan dat resulteren in een beperking van de vrijheid van meningsuiting, de vrijheid om informatie te verwerven, de persvrijheid of het bronnengeheim.

Zoals uiteengezet in B.15.3 dient een koppeling van identificatiegegevens aan andere metadata of aan de inhoud van een communicatie evenwel te zijn gebaseerd op een duidelijke en ondubbelzinnige wetsbepaling, dient zij de materiële en procedurele voorwaarden daarvan na te leven en dient zij in overeenstemming met de grondrechten van de betrokkene te gebeuren.

Een dergelijk onrechtstreeks verband tussen de bestreden afschaffing van de anonimiteit van vooraf betaalde belkaarten en de inhoud van gevoerde communicaties volstaat niet om de bestreden wet als een beperking op de vrijheid van meningsuiting aan te merken. De loutere verzameling van identificatiegegevens van alle eindgebruikers van een elektronische-communicatienetwerk kan in een democratische rechtsstaat niet de vrees rechtvaardigen dat alle communicatie over dat netwerk door de overheid zal worden gemonitord. De bestreden wet kan er bijgevolg op zich niet toe leiden dat personen worden ontmoedigd om hun mening te uiten of om informatie te delen met journalisten of politici.

Het derde onderdeel van het tweede middel is niet gegrond.

Ten aanzien van het derde middel

B.23. In het derde middel voeren de verzoekende partijen aan dat artikel 2, 1°, *c)*, van de bestreden wet de artikelen 10, 11, 12 en 14 van de Grondwet, in samenhang gelezen met de artikelen 6 en 7 van het Europees Verdrag voor de rechten van de mens, de artikelen 48, 49 en 52 van het Handvest, het recht op een eerlijk proces, het vermoeden van onschuld en het strafrechtelijk wettigheidsbeginsel, schendt, doordat het in die bepaling vervatte vermoeden van toerekenbaarheid van de communicatie aan de geïdentificeerde eindgebruiker van de vooraf betaalde belkaart tot gevolg kan hebben dat hij aansprakelijk wordt gesteld voor feiten die hij niet heeft gepleegd.

B.24.1. Artikel 12 van de Grondwet bepaalt :

« De vrijheid van de persoon is gewaarborgd.

Niemand kan worden vervolgd dan in de gevallen die de wet bepaalt en in de vorm die zij voorschrijft.

Behalve bij ontdekking op heterdaad kan niemand worden aangehouden dan krachtens een met redenen omkleed bevel van de rechter dat uiterlijk binnen achtenveertig uren te rekenen van de vrijheidsberoving moet worden betekend en enkel tot voorlopige inhechtenisneming kan strekken ».

Artikel 14 van de Grondwet bepaalt :

« Geen straf kan worden ingevoerd of toegepast dan krachtens de wet ».

Artikel 7 van het Europees Verdrag voor de rechten van de mens bepaalt :

« 1. Niemand kan worden veroordeeld wegens een handelen of nalaten, dat geen strafbaar feit naar nationaal of internationaal recht uitmaakte ten tijde dat het handelen of nalaten geschiedde. Evenmin zal een zwaardere straf worden opgelegd dan die welke ten tijde van het begaan van het strafbare feit van toepassing was.

2. Dit artikel staat niet in de weg aan het vonnis en de straf van iemand die schuldig is aan een handelen of nalaten, hetwelk ten tijde dat het handelen of nalaten geschiedde, een misdrijf was overeenkomstig de algemene rechtsbeginselen welke door de beschaafde volken worden erkend ».

Artikel 49 van het Handvest bepaalt :

« 1. Niemand mag worden veroordeeld wegens een handelen of nalaten dat geen strafbaar feit naar nationaal of internationaal recht uitmaakte ten tijde van het handelen of nalaten. Evenmin mag een zwaardere straf worden opgelegd dan die, die ten tijde van het begaan van het strafbare feit van toepassing was. Indien de wet na het begaan van het strafbare feit in een lichtere straf voorziet, is die van toepassing.

2. Dit artikel staat niet de berechting en bestraffing in de weg van iemand die schuldig is aan een handelen of nalaten dat ten tijde van het handelen of nalaten een misdrijf was volgens de door de volkerengemeenschap erkende algemene beginselen.

3. De zwaarte van de straf mag niet onevenredig zijn aan het strafbare feit ».

B.24.2. Door aan de wetgevende macht de bevoegdheid te verlenen om te bepalen in welke gevallen strafvervolging mogelijk is, waarborgt artikel 12, tweede lid, van de Grondwet aan elke rechtsonderhorige dat geen enkele gedraging strafbaar zal worden gesteld dan krachtens regels aangenomen door een democratisch verkozen beraadslagende vergadering.

Het wettigheidsbeginsel in strafzaken dat uit de voormelde grondwetsbepaling voortvloeit, gaat bovendien uit van de idee dat de strafwet moet worden geformuleerd in bewoordingen op grond waarvan eenieder, op het ogenblik waarop hij een gedrag aanneemt, kan uitmaken of dat gedrag al dan niet strafbaar is. Het vereist dat de wetgever in voldoende nauwkeurige, duidelijke en rechtszekerheid biedende bewoordingen bepaalt welke feiten strafbaar worden gesteld, zodat, enerzijds, diegene die een gedrag aanneemt, vooraf op afdoende wijze kan inschatten wat het strafrechtelijke gevolg van dat gedrag zal zijn en, anderzijds, aan de rechter geen al te grote beoordelingsbevoegdheid wordt gelaten.

Het wettigheidsbeginsel in strafzaken staat evenwel niet eraan in de weg dat de wet aan de rechter een beoordelingsbevoegdheid toekent. Er dient immers rekening te worden gehouden met het algemene karakter van de wetten, de uiteenlopende situaties waarop zij van toepassing zijn en de evolutie van de gedragingen die zij bestraffen.

Aan het vereiste dat een misdrijf duidelijk moet worden omschreven in de wet is voldaan wanneer de rechtzoekende, op basis van de bewoordingen van de relevante bepaling en, indien nodig, met behulp van de interpretatie daarvan door de rechtscolleges, kan weten voor welke handelingen en welke verzuimen hij strafrechtelijk aansprakelijk kan worden gesteld.

Enkel bij het onderzoek van een specifieke strafbepaling is het mogelijk om, rekening houdend met de elementen eigen aan de misdrijven die zij wil bestraffen, te bepalen of de door de wetgever gehanteerde algemene bewoordingen zo vaag zijn dat ze het strafrechtelijk wettigheidsbeginsel zouden schenden.

B.24.3. De bestreden bepaling stelt geen gedragingen strafbaar en bepaalt geen straffen voor specifieke misdrijven. In tegenstelling tot wat de verzoekende partijen aanvoeren, bevat zij evenmin een automatische toerekenbaarheid aan de geïdentificeerde eindgebruiker van een vooraf betaalde belkaart van de misdrijven die worden ontdekt of bewezen na analyse van het gebruik van die belkaart.

Artikel 127, § 1, derde lid, van de wet van 13 juni 2005 bevat slechts het weerlegbare vermoeden dat die eindgebruiker ook degene is die deze belkaart gebruikt. Het strafrechtelijk wettigheidsbeginsel is niet van toepassing op een dergelijke bepaling.

B.25. Artikel 6, lid 2, van het Europees Verdrag voor de rechten van de mens bepaalt :

« Eenieder, die wegens een strafbaar feit wordt vervolgd wordt voor onschuldig gehouden totdat zijn schuld volgens de wet bewezen wordt ».

Artikel 48, lid 1, van het Handvest bepaalt :

« Eenieder tegen wie een vervolging is ingesteld, wordt voor onschuldig gehouden totdat zijn schuld in rechte is komen vast te staan ».

Krachtens die bepalingen wordt eenieder die wegens een strafbaar feit wordt vervolgd voor onschuldig gehouden totdat zijn schuld volgens de wet wordt bewezen.

Wettelijke vermoedens zijn in beginsel niet in strijd met het vermoeden van onschuld (in die zin EHRM, 7 oktober 1988, *Salabiaku t. Frankrijk*, § 28; 20 maart 2001, *Telfner t. Oostenrijk*, § 16). Zij moeten evenwel een redelijk verband van evenredigheid vertonen met het wettig nagestreefde doel (EHRM, 23 juli 2002, *Janosevic t. Zweden*, § 101; 23 juli 2002, *Västberga Taxi Aktiebolag en Vulic t. Zweden*, § 113), waarbij rekening moet worden gehouden met de ernst van de zaak en waarbij het recht van verdediging moet worden gevrijwaard (EHRM, 4 oktober 2007, *Anghel t. Roemenië*, § 60).

B.26.1. Initieel bepaalde het voorontwerp dat tot de bestreden wet heeft geleid, dat de geïdentificeerde persoon « verantwoordelijk » is voor het gebruik van de elektronische-communicatiedienst die hem wordt verstrekt. In het advies nr. 59.423/4 van 15 juni 2016 heeft de Raad van State, afdeling wetgeving, daarover het volgende opgemerkt :

« Wat het ontworpen artikel 127, § 1, derde lid, betreft, ziet de afdeling Wetgeving niet in wat de concrete strekking is van de ontworpen regel, die bepaalt dat de geïdentificeerde natuurlijke of rechtspersoon ' verantwoordelijk ' is voor het gebruik van de elektronische-communicatiedienst die aan hem wordt verstrekt. Wat wordt daarmee precies bedoeld ? Gaat het om de contractuele aansprakelijkheid ten aanzien van de operator, om een aquiliaanse aansprakelijkheid ten aanzien van derden, of nog om een strafrechtelijke verantwoordelijkheid ?

De ontworpen tekst moet worden herzien om de inhoud en de draagwijdte van de in het vooruitzicht gestelde verantwoordelijkheid te preciseren, inzonderheid wanneer die term een of andere strafrechtelijke verantwoordelijkheid dekt » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1964/001, pp. 46-47).

Gelet op dat advies heeft de wetgever elke verwijzing naar de « verantwoordelijkheid » van de eindgebruiker uit het ontwerp geschrapt. In de parlementaire voorbereiding heeft hij de uiteindelijke versie van de bestreden bepaling als volgt toegelicht :

« Het nieuwe, ingevoerde lid is grondig herzien na het advies van de Raad van State, die van oordeel was dat hij niet de concrete draagwijdte van de ontwerpregel inzag.

Het principe dat de geïdentificeerde persoon in principe de daadwerkelijke gebruiker is van de elektronische-communicatiedienst (behoudens tegenbewijs) maakt het mogelijk te voorkomen dat een persoon zichzelf identificeert in plaats van een derde die de elektronische-communicatiedienst effectief gebruikt, om de identiteit te verbergen » (*ibid.*, p. 9).

B.26.2. De bestreden bepaling vestigt bijgevolg geen automatische strafrechtelijke verantwoordelijkheid of objectieve aansprakelijkheid van de geïdentificeerde eindgebruiker van een vooraf betaalde belkaart voor het gebruik dat een derde daarvan maakt. Zij heeft voornamelijk een waarschuwingsfunctie, aangezien zij het uitgangspunt van elk strafrechtelijk onderzoek en van elk onderzoek door de inlichtingen- en veiligheidsdiensten in herinnering brengt, namelijk het uitgangspunt dat de eigenaar of gewoonlijke gebruiker van een voorwerp vermoedelijk degene is die het heeft gebruikt om een misdrijf te plegen of om de nationale veiligheid te bedreigen. De onderzoekers verlaten dat uitgangspunt zodra het wordt ontkracht door de verzamelde bewijselementen.

Voorts dient de bestreden bepaling, zoals uiteengezet in B.16.11.2, in samenhang te worden gelezen met de artikelen 5 en 6 van het koninklijk besluit van 27 november 2016, die de overdraagbaarheid van de vooraf betaalde belkaart beperken en de eindgebruiker verplichten om het verlies of de diefstal ervan binnen 24 uur aan de operator te melden. Het geheel van die bepalingen draagt bij aan de pertinentie van artikel 127 van de wet van 13 juni 2005, aangezien zij de identificeerbaarheid van de werkelijke gebruiker van een vooraf betaalde belkaart beoogt te vergemakkelijken.

B.26.3. De bestreden bepaling houdt aldus verband met de doelstellingen die de wetgever met artikel 127 van de wet van 13 juni 2005 nastreeft, met name in noodsituaties en onderzoeken waarmee tijdsdruk gepaard gaat.

B.26.4. De bestreden bepaling speelt bovendien vaak in het kader van misdrijven of bedreigingen van de nationale veiligheid die ernstige gevolgen kunnen hebben voor de fysieke integriteit van personen of aanzienlijke maatschappelijke onrust kunnen veroorzaken.

B.26.5. De geïdentificeerde eindgebruiker beschikt over verschillende mogelijkheden om zich te verdedigen tegen strafrechtelijke vervolgingen die zouden kunnen voortvloeien uit het gebruik dat een derde van zijn vooraf betaalde kaart heeft gemaakt. Indien hij aan de onderzoekers meldt wie gebruik heeft gemaakt van zijn vooraf betaalde belkaart, dienen zij diens betrokkenheid te onderzoeken.

De bestreden bepaling stelt overigens slechts een weerlegbaar vermoeden in, dat door de beklaagde met alle middelen van recht kan worden weerlegd. Zij verbiedt hem niet om alle feitelijke elementen aan te dragen die zijn betrokkenheid bij de gepleegde misdrijven of bij de onderzochte bedreigingen voor de nationale veiligheid ontkrachten.

Daarnaast doet de bestreden bepaling geen afbreuk aan het beginsel dat het in een strafproces aan het openbaar ministerie toekomt de schuld van de beklaagde te bewijzen. Het staat aan de strafrechter de bewijswaarde van alle bewijselementen, met inbegrip van de uitleg van de beklaagde, te onderzoeken en daarbij diens recht op een eerlijk proces te eerbiedigen.

Aangezien de bestreden bepaling aldus geen afbreuk doet aan het recht van verdediging van de beklaagde, brengt zij evenmin het vermoeden van onschuld in het gedrang.

B.26.6. In tegenstelling tot hetgeen de verzoekende partijen aanvoeren, geldt het voorgaande evenzeer voor de betrokkenheid van de geïdentificeerde eindgebruiker bij de terroristische misdrijven vermeld in de artikelen 137 tot 141*ter* van het Strafwetboek. Hij kan slechts als mededader of medeplichtige van dergelijke misdrijven worden veroordeeld indien het openbaar ministerie alle constitutieve elementen van die misdrijven, met inbegrip van het intentionele element, te zijnen aanzien bewijst.

Het te goeder trouw ter beschikking stellen van een vooraf betaalde belkaart door een eindgebruiker die niet kon vermoeden dat zij zou worden gebruikt om een dergelijk misdrijf te plegen of voor te bereiden, kan op zich geen strafrechtelijke veroordeling verantwoorden.

B.26.7. Onder voorbehoud van de in B.26.2 en B.26.6 vermelde interpretaties is het derde middel niet gegrond.

Ten aanzien van het vierde middel

B.27.1. In het vierde middel voeren de verzoekende partijen aan dat artikel 3 van de bestreden wet de artikelen 10, 11 en 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8 en 52 van het Handvest, met de artikelen 2, *a)*, 6, 13 en 22 van de richtlijn 95/46/EG en met de artikelen 1, 2, 3, 5, 6, 9 en 15 van de richtlijn 2002/58/EG, schendt. Het middel valt uiteen in vijf onderdelen.

B.27.2. In het eerste onderdeel voeren zij aan dat de bestreden bepaling de inlichtingen- en veiligheidsdiensten toegang geeft tot de krachtens artikel 127 van de wet van 13 juni 2005 verzamelde identificatiegegevens, zonder die toegang te beperken tot ernstige misdrijven.

In het tweede onderdeel voeren zij aan dat die toegang van de inlichtingen- en veiligheidsdiensten niet wordt onderworpen aan een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit.

In het derde onderdeel voeren zij aan dat de bestreden bepaling de materiële en procedurele voorwaarden van die toegang onvoldoende preciseert.

In het vierde onderdeel voeren zij aan dat de bestreden bepaling de inlichtingen- en veiligheidsdiensten die toegang hebben tot de krachtens artikel 127 van de wet van 13 juni 2005 verwerkte identificatiegegevens, niet verplicht om de betrokkene daarvan op de hoogte te brengen opdat hij zijn recht op een daadwerkelijke rechterlijke controle kan uitoefenen.

In het vijfde onderdeel voeren zij aan dat de bestreden bepaling niet uitsluit dat buitenlandse inlichtingen- en veiligheidsdiensten toegang tot die gegevens krijgen.

Gelet op hun onderlinge samenhang dienen die onderdelen samen te worden behandeld.

B.28.1. Krachtens artikel 1, lid 3, van de richtlijn 2002/58/EG is die richtlijn « niet van toepassing op activiteiten die niet onder het EG-Verdrag vallen, zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie, en in geen geval op activiteiten die verband houden met de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economische welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de activiteiten van de staat op strafrechtelijk gebied ».

Krachtens artikel 2, lid 2, *a)*, van de AVG is die verordening « niet van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen ». Krachtens artikel 2, lid 2, *d)*, van de AVG is zij evenmin van toepassing op de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

Bij zijn arrest van 6 oktober 2020 in zake *La Quadrature du Net e.a.* (C-511/18, C-512/18 en C-520/18) heeft de grote kamer van het Hof van Justitie geoordeeld :

« 135. In dit verband moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten ».

B.28.2. De bestreden bepaling voegt in de wet van 30 november 1998 een nieuw artikel 16/2, § 2, in. Krachtens die bepaling kunnen de inlichtingen- en veiligheidsdiensten, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een bank of financiële instelling om over te gaan tot het identificeren van de eindgebruiker van een vooraf betaalde belkaart op basis van de referentie van een elektronische banktransactie die verband houdt met die belkaart en die voorafgaand is meegedeeld door de betrokken onderneming.

B.28.3. Aangezien de bestreden bepaling slechts van toepassing is in het kader van de opdrachten van de inlichtingen- en veiligheidsdiensten, valt zij buiten het toepassingsgebied van het Europees Unierecht. Bijgevolg is het middel onontvankelijk in zoverre het de schending aanvoert van de aangevoerde bepalingen van het Handvest, van de AVG of van de richtlijn 2002/58/EG.

B.29.1. De toegang van een overheid tot bankgegevens valt onder het toepassingsgebied van het recht op eerbiediging van het privéleven, ongeacht of die gegevens privacygevoelig zijn en ongeacht of zij verband houden met de beroepsuitoefening (EHRM, 7 juli 2005, *M.N. e.a. t. San Marino*, §§ 51-55; 1 december 2015, *Brito Ferrinho Bexiga Villa-Nova t. Portugal*, § 44; 27 april 2017, *Sommer t. Duitsland*, § 48).

B.29.2. De toegang van de overheid tot bankgegevens dient gebaseerd te zijn op een specifieke wettelijke machtiging die het voorwerp ervan, alsook de drempel om er zich toegang toe te verschaffen, duidelijk en ondubbelzinnig afbakent. Dat voorwerp dient beperkt te zijn tot hetgeen noodzakelijk is in het licht van de nagestreefde wettige doelstelling, aangezien een te ruime toegang tot bankgegevens de overheid zou toelaten zich een gedetailleerd beeld te vormen van het privéleven van de betrokkene. De overheid mag slechts toegang tot dergelijke gegevens hebben indien zij over concrete aanwijzingen beschikt dat de houder van de bankrekening betrokken is bij een misdrijf. Tevens dient de wet te voorzien in maatregelen tegen misbruik, waaronder de waarborg dat de gegevens niet langer worden bewaard dan noodzakelijk in het licht van het gevoerde onderzoek. Tot slot dient een daadwerkelijk rechterlijk toezicht te bestaan op de naleving van die materiële en procedurele voorwaarden (EHRM, 27 april 2017, *Sommer t. Duitsland*, §§ 57-63).

B.30.1. De bestreden bepaling preciseert welke diensten over de in B.28.2 bedoelde machtiging beschikken en welke instellingen tot medewerking gehouden zijn.

Zij bakent ook op tweevoudige wijze de doelstelling van de bestreden maatregel af. Ten eerste beoogt hij hetzij de in artikel 127 van de wet van 13 juni 2005 bedoelde eindgebruiker van een vooraf betaalde belkaart te identificeren, hetzij de vooraf betaalde belkaart te identificeren die door een bepaald persoon wordt gebruikt. Ten tweede moet die identificatie passen in het kader van de opdrachten van de inlichtingen- en veiligheidsdiensten.

B.30.2. Het voorwerp van de onderzoeksdaad is beperkt tot één specifieke banktransactie, namelijk degene waarmee een vooraf betaalde belkaart is aangekocht. Een dergelijke onderzoeksdaad laat de inlichtingen- en veiligheidsdiensten slechts toe identificatiegegevens te verwerven, maar verschaft hen op zich geen verkeers- of locatiegegevens, noch toegang tot de gevoerde communicaties.

De bestreden bepaling laat hun evenmin toe alleen met die onderzoeksdaad andere financiële informatie met betrekking tot de houder van de bankrekening te verkrijgen. Aldus maakt zij het hun niet mogelijk zich louter aan de hand van de verworven identificatiegegevens een beeld te vormen van het bestedingsgedrag of enig ander privacygevoelig element met betrekking tot de houder van de bankrekening.

Zoals uiteengezet in B.15.3 kunnen die identificatiegegevens vervolgens weliswaar worden gekoppeld aan andere gegevens en kan de bestreden bepaling aldus bijdragen aan het vrijgeven van dergelijke gevoelige informatie, maar die informatie dient dan te worden verzameld aan de hand van andere onderzoeksdaden, die op hun beurt de toepasselijke wetgeving en de grondrechten van de betrokkene moeten eerbiedigen.

B.30.3. Zoals uiteengezet in B.3.3, kan de identificatie op grond van de bestreden bepaling noodzakelijk zijn naar gelang van de identificatiemethode waarvoor de eindgebruiker bij de aankoop van de vooraf betaalde belkaart heeft gekozen.

Indien hij bij de aankoop van de vooraf betaalde belkaart kiest voor de identificatie op grond van de onlinebetalingstransactie, kunnen de inlichtingen- en veiligheidsdiensten hem slechts identificeren indien zij over de referentie van de elektronische banktransactie beschikken en deze kunnen koppelen aan zowel de belkaart als de identiteit van de eindgebruiker (*Parl. St.*, Kamer, 2015-2016, DOC 54-1964/001, pp. 14-16). Die identificatiemethode wordt geregeld in artikel 17 van het koninklijk besluit van 27 november 2016, dat bepaalt :

« § 1. De betrokken onderneming kan de eindgebruiker identificeren op basis van een elektronische betalingstransactie online specifiek om een voorafbetaalde kaart aan te kopen of te herladen.

Deze methode is onderworpen aan de volgende voorwaarden :

1° de betalingstransactie moet worden afgehandeld via een betalingsdienstaanbieder zoals bedoeld in art. I.9. 2°, *a)*, *b)*, *c)*, en *d)* van het Wetboek van Economisch Recht;

2° de betalingsdienstaanbieder is onderworpen aan de Wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme;

3° er moet een nieuwe identificatie worden uitgevoerd binnen de 18 maanden die volgen op de betalingstransactie die is gelinkt aan de voorafbetaalde kaart;

4° op een online formulier van de betrokken onderneming vult de eindgebruiker op zijn minst zijn naam, zijn voornaam en geboortedatum en -plaats in.

§ 2. De betrokken onderneming slaat de referentie van de betalingstransactie en de gegevens van het online formulier op ».

B.30.4. Aangezien de bestreden bepaling de inlichtingen- en veiligheidsdiensten slechts machtigt om de bestreden onderzoeksdaad te stellen « in het belang van de uitoefening van hun opdrachten », dienen zij daarbij steeds te beschikken over concrete aanwijzingen dat de identificatie van de eindgebruiker van een vooraf betaalde belkaart noodzakelijk is in het kader van de opdrachten die limitatief worden opgesomd in artikel 7 (Veiligheid van de Staat) en artikel 11 (Algemene Dienst Inlichting en Veiligheid) van de wet van 30 november 1998. Aangezien die opdrachten alle betrekking hebben op vitale belangen van de Natie, is bij het nemen van die maatregel steeds minstens een dreiging aanwezig dat zich een gebeurtenis met zeer ingrijpende maatschappelijke gevolgen zou voordoen.

B.30.5. De bestreden bepaling waarborgt dat de vordering uitgaat van het diensthoofd of zijn afgevaardigde en dat zij schriftelijk gebeurt of binnen 24 uur schriftelijk wordt bevestigd. Daarnaast vereist artikel 16/2, § 4, van de wet van 30 november 1998 dat de inlichtingen- en veiligheidsdiensten een register bijhouden van alle gevorderde identificaties. Zij dienen die lijst maandelijks te bezorgen aan het Vast Comité I.

De verzoekende partijen voeren in dat verband aan dat de bestreden bepaling niet vereist dat de vordering van het diensthoofd of zijn afgevaardigde met redenen wordt omkleed. Een dergelijke verplichting zou het geheime karakter en de effectiviteit van de door de inlichtingen- en veiligheidsdiensten gevoerde onderzoeken evenwel in het gedrang brengen.

B.30.6. De bestreden bepaling waarborgt geen specifiek rechterlijk toezicht op de bestreden onderzoeksmaatregel. Zoals in B.14.3 werd uiteengezet, volstaan inzake de verwerking van en de toegang tot loutere identificatiegegevens evenwel de gemeenrechtelijke rechtsmiddelen (EHRM, 30 januari 2020, *Breyer t. Duitsland*, § 106). De betrokkene beschikt in dat verband over de in B.16.10 vermelde rechtsmiddelen.

B.30.7. Aangezien de bestreden onderzoeksdaad een gewone methode voor het verzamelen van gegevens is, zijn het in artikel 43/1 van de wet van 30 november 1998 bedoelde toezicht door de bestuurlijke commissie en de in de artikelen 43/2 tot 43/8 van de wet van 30 november 1998 bedoelde controle *a posteriori* door het Vast Comité I er niet op van toepassing.

Gelet op de beperkte draagwijdte van de bestreden bepaling, gelet op het fundamentele belang van de nationale veiligheid, gelet op het feit dat de inlichtingen- en veiligheidsdiensten met de bestreden maatregel slechts identificatiegegevens kunnen verwerven en gelet op de in B.30.5 vermelde waarborgen, volstaat dat gebrek aan toezicht niet om te besluiten dat de bestreden bepaling het recht op eerbiediging van het privéleven zou schenden.

B.30.8. De verzoekende partijen voeren voorts aan dat het Hof de wetgever bij zijn arresten nrs. 145/2011 van 22 september 2011 en 41/2019 van 14 maart 2019 heeft verplicht om te voorzien in een actieve kennisgevingsplicht vanwege de inlichtingen- en veiligheidsdiensten aan eenieder die het voorwerp heeft uitgemaakt van een onderzoek door die diensten zodra het geheim van het onderzoek is opgeheven.

Het Hof heeft dit evenwel slechts vereist voor de uitzonderlijke methoden van verzamelen van gegevens bedoeld in de artikelen 18/12, 18/14 en 18/17 van de wet van 30 november 1998, die de inlichtingen- en veiligheidsdiensten toelaten kennis te nemen van de inhoud van communicaties. Het overwoog daarbij dat die methoden het meest ingrijpend zijn voor het privéleven van de betrokkene. Het heeft dit daarentegen niet vereist voor de gewone methodes van verzamelen van gegevens, noch voor onderzoeksdaden die slechts betrekking hebben op het verwerven van identificatiegegevens.

B.30.9. In zoverre de verzoekende partijen tot slot aanvoeren dat de bestreden bepaling toelaat dat de inlichtingen- en veiligheidsdiensten de verworven identificatiegegevens kunnen delen met buitenlandse inlichtingen- en veiligheidsdiensten, volstaat het vast te stellen dat een dergelijke samenwerking niet het voorwerp uitmaakt van de bestreden bepaling, maar van het door hen niet bestreden artikel 20 van de wet van 30 november 1998.

B.30.10. Onder voorbehoud van de in B.30.4 vermelde interpretatie is het vierde middel niet gegrond.

Om die redenen,

het Hof

- vernietigt artikel 2 van de wet van 1 september 2016 « tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst », zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen;

- handhaaft de gevolgen van de vernietigde bepaling tot de inwerkingtreding van een wetskrachtige norm waarin die identificatiegegevens en identificatiedocumenten worden opgesomd en uiterlijk tot en met 31 december 2022;

- verwerpt het beroep voor het overige, onder voorbehoud van de in B.8.7.3, B.16.6, B.16.8.5, B.16.8.7, B.26.2, B.26.6 en B.30.4 vermelde interpretaties.

Aldus gewezen in het Nederlands, het Frans en het Duits, overeenkomstig artikel 65 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, op 18 november 2021.

De griffier, De voorzitter,

P.-Y. Dutilleux L. Lavrysen

COUR CONSTITUTIONNELLE

[2021/205605]

Extrait de l'arrêt n° 158/2021 du 18 novembre 2021

Numéro du rôle : 6672

En cause : le recours en annulation de la loi du 1er septembre 2016 « portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité », introduit par Patrick Van Assche et autres.

La Cour constitutionnelle,

composée des présidents L. Lavrysen et P. Nihoul, des juges J.-P. Moerman, T. Giet, R. Leysen, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne et D. Pieters, et, conformément à l'article 60*bis* de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, du président émérite F. Daoût et de la juge émérite T. Merckx-Van Goey, assistée du greffier P.-Y. Dutilleux, présidée par le président L. Lavrysen,

après en avoir délibéré, rend l'arrêt suivant :

I. *Objet du recours et procédure*

Par requête adressée à la Cour par lettre recommandée à la poste le 7 juin 2017 et parvenue au greffe le 8 juin 2017, un recours en annulation de la loi du 1er septembre 2016 « portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité » (publiée au *Moniteur belge* du 7 décembre 2016) a été introduit par Patrick Van Assche, Christel Van Akeleyen et Karina De Hoog, assistés et représentés par Me D. Pattyn, avocat au barreau de Flandre occidentale.

(...)

II. *En droit*

(...)

B.1.1. La loi du 1er septembre 2016 « portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité » (ci-après : la loi attaquée) dispose :

« CHAPITRE 1er. - Objet

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

CHAPITRE 2. - Modifications de la loi du 13 juin 2005 relative aux communications électroniques

Art. 2. Dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, modifié par les lois des 4 février 2010, 10 juillet 2012, 27 mars 2014 et 29 mai 2016, les modifications suivantes sont apportées :

1° dans le paragraphe 1er, les modifications suivantes sont apportées :

a) dans l'alinéa 1er, les mots ' aux canaux de vente de services de communications électroniques, aux entreprises fournissant un service d'identification ' sont insérés entre les mots ' visés à l'article 126, § 1er, alinéa 1er, ' et les mots ' ou aux utilisateurs finals ';

b) dans le texte néerlandais, à l'alinéa 1er, les mots ' de verkoopkanalen van elektronische-communicatiediensten, de ondernemingen die een identificatiedienst verstrekken ' sont insérés entre les mots ' bedoeld in artikel 126, § 1, eerste lid, ' et les mots ' of aan de eindgebruikers ';

c) sept alinéas rédigés comme suit sont insérés entre les alinéas 1er et 2 :

' Pour ce qui concerne l'identification de l'utilisateur final, l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, est le responsable du traitement au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.

Lorsque l'utilisateur final présente un document d'identification comprenant le numéro de registre national, l'opérateur, le fournisseur visé à l'article 126, § 1er, alinéa 1er, le canal de vente de services de communications électroniques ou l'entreprise fournissant un service d'identification collecte ce numéro.

Le canal de vente de services de communications électroniques ne conserve pas de données ou de documents d'identification, qui sont transmis à l'opérateur, au fournisseur visé à l'article 126, § 1er, alinéa 1er ou à l'entreprise fournissant un service d'identification.

Si une introduction directe dans les systèmes informatiques de l'opérateur, du fournisseur visé à l'article 126, § 1er, alinéa 1er ou de l'entreprise fournissant un service d'identification n'est pas possible, le canal de vente de services de communications électroniques peut faire une copie du document d'identification, dont la carte d'identité électronique belge, mais cette copie est détruite au plus tard après l'activation du service de communications électroniques.

L'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er conserve une copie des documents d'identification autres que la carte d'identité électronique belge.

Les données et documents d'identification collectés sont conservés conformément à l'article 126, § 3, alinéa 1er. '

2° le paragraphe 3 est complété par l'alinéa suivant :

' Les utilisateurs finals non identifiés de cartes prépayées achetées avant l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, qui sont définis par cet arrêté royal, s'identifient dans le délai fixé par l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, ce délai ne pouvant excéder six mois après la publication de l'arrêté royal visé au paragraphe 1er. L'interdiction visée au paragraphe 2 ne s'applique qu'après la fin du délai accordé à l'utilisateur final pour s'identifier. '

3° dans le paragraphe 4, les modifications suivantes sont apportées :

a) les mots ' ou un fournisseur visé à l'article 126, § 1er, alinéa 1er, ' sont insérés entre les mots ' un opérateur ' et les mots ' ne respecte pas les mesures techniques et administratives qui lui sont imposées ';

b) dans le texte néerlandais, les mots ' binnen de door de Koning vastgestelde termijn ' sont abrogés;

c) dans le texte néerlandais, les mots ' of een aanbieder bedoeld in artikel 126, § 1, eerste lid, ' sont insérés entre les mots ' een operator ' et les mots ' niet voldoet aan de hem opgelegde technische en administratieve maatregelen ';

d) les mots ' dans le délai fixé ' sont remplacés par les mots ' par le présent article ou ';

e) dans le texte néerlandais, les mots ' door dit artikel of door de Koning ' sont insérés entre les mots ' niet voldoen aan de hen ' et les mots ' opgelegde technische en administratieve maatregelen ';

4° dans le paragraphe 5, les modifications suivantes sont apportées :

a) dans l'alinéa 1er, les mots ' et les fournisseurs visés à l'article 126, § 1er, alinéa 1er, ' sont insérés entre les mots ' Les opérateurs ' et les mots ' déconnectent les utilisateurs finals ';

b) dans le texte néerlandais, dans l'alinéa 1er, les mots ' en de aanbieders bedoeld in artikel 126, § 1, eerste lid, ' sont insérés entre les mots ' De operatoren ' et les mots ' sluiten de eindgebruikers ';

c) dans l'alinéa 1er, les mots ' dans le délai fixé ' sont remplacés par les mots ' par le présent article ou ';

d) dans le texte néerlandais, à l'alinéa 1er, les mots ' binnen de door de Koning vastgestelde termijn ' sont abrogés;

e) dans le texte néerlandais, à l'alinéa 1er, les mots ' door dit artikel of door de Koning ' sont insérés entre les mots ' niet voldoen aan de hen ' et les mots ' opgelegde technische en administratieve maatregelen ';

f) l'alinéa 2 est abrogé.

CHAPITRE 3. - Modifications de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Art. 3. Dans l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, inséré par la loi du 5 février 2016, les modifications suivantes sont apportées :

1° les actuels alinéas 1er à 4 formeront le paragraphe 1er et le mot ' chef ' est chaque fois remplacé par le mot ' dirigeant ';

2° il est inséré un paragraphe 2, rédigé comme suit :

' § 2. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée visée dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d'une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.

La réquisition est effectuée par écrit par le dirigeant de service ou son délégué. En cas d'urgence, le dirigeant de service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite.

Toute banque et toute institution financière qui est requise donne sans délai au dirigeant de service ou à son délégué les données qui ont été demandées.

Les données d'identification que les services de renseignement et de sécurité reçoivent dans le cadre de l'exercice de la méthode visée au présent paragraphe, se limitent aux données d'identification visées au paragraphe 1er. ';

3° l'actuel alinéa 5 formera le paragraphe 3;

4° dans le texte néerlandais, dans l'actuel sixième alinéa, dont le texte formera le paragraphe 4, les mots ' de betrokken inlichtingen- en veiligheidsdiensten ' sont remplacés par les mots ' de betrokken inlichtingen- en veiligheidsdienst ' et dans le texte français, les mots ' et de sécurité ' sont insérés entre les mots ' service de renseignement ' et le mot ' concerné ' ».

B.1.2. La loi attaquée fait partie des mesures de lutte contre le terrorisme qui ont été prises à la suite des attentats terroristes commis à Paris le 13 novembre 2015 et à Bruxelles le 22 mars 2016 (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, p. 2). L'article 2 de la loi attaquée modifie l'article 127 de la loi du 13 juin 2005 « relative aux communications électroniques » (ci-après : la loi du 13 juin 2005) en vue de la suppression de l'anonymat des cartes de téléphonie mobile prépayées. L'article 3 de la loi attaquée modifie l'article 16/2 de la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité » (ci-après : la loi du 30 novembre 1998) afin de permettre l'identification de l'utilisateur final d'une carte de téléphonie mobile prépayée sur la base de la transaction bancaire en ligne qui a été effectuée pour l'acheter.

B.2.1. L'article 127 de la loi du 13 juin 2005, modifié par l'article 2 de la loi attaquée, dispose :

« § 1er. Le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs, aux fournisseurs visés à l'article 126, § 1er, alinéa 1er, aux canaux de vente de services de communications électroniques, aux entreprises fournissant un service d'identification ou aux utilisateurs finals, en vue de permettre :

1° l'identification de la ligne appelante dans le cadre d'un appel d'urgence;

2° l'identification de l'utilisateur final, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46*bis*, 88*bis* et 90*ter* à 90*decies* du Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Pour ce qui concerne l'identification de l'utilisateur final, l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, est le responsable du traitement au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.

Lorsque l'utilisateur final présente un document d'identification comprenant le numéro de registre national, l'opérateur, le fournisseur visé à l'article 126, § 1er, alinéa 1er, le canal de vente de services de communications électroniques ou l'entreprise fournissant un service d'identification collecte ce numéro.

Le canal de vente de services de communications électroniques ne conserve pas de données ou de documents d'identification, qui sont transmis à l'opérateur, au fournisseur visé à l'article 126, § 1er, alinéa 1er ou à l'entreprise fournissant un service d'identification.

Si une introduction directe dans les systèmes informatiques de l'opérateur, du fournisseur visé à l'article 126, § 1er, alinéa 1er ou de l'entreprise fournissant un service d'identification n'est pas possible, le canal de vente de services de communications électroniques peut faire une copie du document d'identification, dont la carte d'identité électronique belge, mais cette copie est détruite au plus tard après l'activation du service de communications électroniques.

L'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er conserve une copie des documents d'identification autres que la carte d'identité électronique belge.

Les données et documents d'identification collectés sont conservés conformément à l'article 126, § 3, alinéa 1er.

Le Roi fixe, après l'avis de l'Institut, les tarifs rétribuant la collaboration des opérateurs et des fournisseurs visés à l'article 126, § 1er, alinéa 1er, aux opérations visées à l'alinéa 1er, 2° ainsi que le délai dans lequel les opérateurs ou les abonnés doivent donner suite aux mesures imposées.

§ 2. Sont interdites : la fourniture ou l'utilisation d'un service ou d'un équipement qui rend difficile ou impossible l'exécution des opérations visées au § 1er, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.

§ 3. Jusqu'à ce que les mesures visées au § 1er entrent en vigueur, l'interdiction visée au § 2 ne s'applique pas aux services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.

Les utilisateurs finals non identifiés de cartes prépayées achetées avant l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, qui sont définis par cet arrêté royal, s'identifient dans le délai fixé par l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, ce délai ne pouvant excéder six mois après la publication de l'arrêté royal visé au paragraphe 1er. L'interdiction visée au paragraphe 2 ne s'applique qu'après la fin du délai accordé à l'utilisateur final pour s'identifier.

§ 4. Si un opérateur ou un fournisseur visé à l'article 126, § 1er, alinéa 1er, ne respecte pas les mesures techniques et administratives qui lui sont imposées par le présent article ou par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.

§ 5. Les opérateurs et les fournisseurs visés à l'article 126, § 1er, alinéa 1er, déconnectent les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées par le présent article ou par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces utilisateurs finals ne sont en aucune manière indemnisés pour la déconnexion ».

B.2.2. L'article 127 de la loi du 13 juin 2005 s'est toujours fondé sur la prémisse selon laquelle tous les utilisateurs finaux de réseaux de communications électroniques doivent être identifiables. À l'origine, cette disposition n'imposait des obligations qu'aux opérateurs, aux fournisseurs et aux utilisateurs finaux de ces services. L'article 127, § 1er, alinéa 1er, confère une habilitation générale au Roi pour fixer les mesures techniques et administratives en vue de permettre cette identifiabilité.

Cette identifiabilité sert deux objectifs. Premièrement, elle vise à contribuer au bon fonctionnement des services d'urgence en permettant l'identification de la ligne appelante d'un appel d'urgence (article 127, § 1er, alinéa 1er, 1o). Deuxièmement, elle contribue au repérage, à la localisation, aux écoutes, à la prise de connaissance et à l'enregistrement des communications privées aux conditions prévues par les articles 46*bis*, 88*bis* et 90*ter* à 90*decies* du Code d'instruction criminelle et par la loi du 30 novembre 1998 (article 127, § 1er, alinéa 1er, 2o).

L'article 127, § 2, de la loi du 13 juin 2005 interdit la fourniture ou l'utilisation de services ou d'équipements qui rendent l'identifiabilité difficile, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.

L'article 127, § 3, de la même loi prévoyait initialement une exception temporaire à cette interdiction pour les utilisateurs finaux de cartes de téléphonie mobile prépayées. Ces utilisateurs finaux étaient dispensés de l'obligation d'être identifiables tant que le Roi n'avait pas encore pris les mesures techniques et administratives visées à l'article 127, § 1er.

B.2.3. L'article 2 de la loi attaquée a modifié l'article 127 de la loi du 13 juin 2005 sur différents points. Premièrement, il en a étendu le champ d'application en imposant certaines des obligations contenues dans cet article également aux canaux de vente de services de communications électroniques et aux entreprises fournissant un service d'identification.

Deuxièmement, cette disposition a ancré dans la loi un certain nombre d'aspects de l'identification de l'utilisateur final. Ainsi, l'opérateur et le fournisseur sont désignés comme les responsables du traitement des données à caractère personnel (article 127, § 1er, alinéa 2). Cette disposition indique également que, sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques (article 127, § 1er, alinéa 3), que l'identification doit s'effectuer sur la base d'un document d'identification comportant le numéro de registre national (article 127, § 1er, alinéa 4) et que le canal de vente de services de communications électroniques ne peut pas conserver de copies des données ou des documents d'identification qu'il transmet à l'opérateur (article 127, § 1er, alinéas 5 à 7).

Troisièmement, cette disposition comporte quelques habilitations spécifiques au Roi, telles que l'habilitation conférée au Roi dans le nouvel article 127, § 1er, alinéa 8, de la loi du 13 juin 2005, par laquelle le Roi fixe la rétribution des opérateurs et des fournisseurs dans les cas où ils doivent contribuer à l'identification des utilisateurs finaux de leurs services, ainsi que le délai dans lequel les opérateurs et les abonnés doivent donner suite aux mesures imposées. Le nouvel alinéa 2 de l'article 127, § 3, de la loi du 13 juin 2005 habilite le Roi à fixer le délai dans lequel l'utilisateur final d'une carte de téléphonie mobile prépayée achetée avant l'entrée en vigueur de la loi attaquée doit s'identifier. Ce délai ne peut pas excéder six mois après la publication de l'arrêté royal visé à l'article 127, § 1er, de la même loi. En vertu du nouvel article 127, § 3, alinéa 2, de la loi du 13 juin 2005, l'anonymat des cartes de téléphonie mobile prépayées n'est levé qu'après la fin de ce délai.

B.2.4. Le Roi a mis à exécution l'article 127 de la loi du 13 juin 2005, du moins pour ce qui concerne les services de communications électroniques qui sont offerts sur la base d'une carte de téléphonie mobile prépayée, par l'arrêté royal du 27 novembre 2016 « relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée » (ci-après : l'arrêté royal du 27 novembre 2016).

L'article 2, 4o, de cet arrêté royal définit le document d'identification valide comme « la carte d'identité belge ou d'un État membre de l'Union européenne, la carte électronique belge pour étrangers, le document reprenant le numéro visé à l'art 8, § 1er, 2o, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale ou à l'article 2, alinéa 2, de la loi du 8 août 1983 organisant un registre national des personnes physiques ou le passeport international ou le document officiel remplaçant, à titre provisoire, un des documents susmentionnés qui a été perdu ou volé, pour autant que le document d'identification soit original, lisible et valide ».

Les articles 3 à 6 de l'arrêté royal du 27 novembre 2016 imposent des obligations aux utilisateurs finaux de cartes de téléphonie mobile prépayées. Ils doivent s'identifier auprès de l'opérateur à chaque fois que celui-ci le demande. Lorsqu'ils achètent une nouvelle carte de téléphonie mobile prépayée, ils communiquent leur identité à l'opérateur au plus tard lors de l'activation de cette carte selon une des méthodes d'identification valides. Il leur est en principe interdit de céder leur carte prépayée à des tiers, sauf dans les cas et aux conditions fixés à l'article 5 de l'arrêté royal. S'ils perdent leur carte prépayée ou si celle-ci est volée, ils doivent en informer l'opérateur dans les 24 heures.

Les articles 7 à 9 du même arrêté royal imposent des obligations aux opérateurs. Ces derniers devaient identifier avant le 7 juin 2017 tous les utilisateurs finaux de cartes prépayées qui avaient été achetées avant l'entrée en vigueur, le 17 décembre 2016, de cet arrêté royal. Depuis l'entrée en vigueur de cet arrêté royal, ils ne peuvent plus activer de nouvelles cartes prépayées si l'utilisateur final n'a pas encore été identifié. S'ils sont informés par l'utilisateur final de la perte ou du vol de la carte de téléphonie mobile prépayée, ils doivent la rendre immédiatement inutilisable.

B.2.5. Les articles 9 à 12 du même arrêté royal définissent la manière dont l'utilisateur final d'une carte de téléphonie mobile prépayée doit être identifié et dont ses données d'identification sont traitées. L'opérateur, le fournisseur d'un service d'identification ou le canal de vente de services de communications électroniques collectent ces données en lisant électroniquement la carte d'identité électronique belge ou en faisant un scan, une photo ou une copie de celle-ci, en ce compris de la photo se trouvant sur cette carte et du numéro de cette carte. Avant l'activation de la carte de téléphonie mobile prépayée, l'opérateur doit contrôler si la carte d'identité présentée n'a pas été volée ou ne pas fait l'objet d'une fraude.

L'opérateur conserve la méthode d'identification utilisée pour identifier l'utilisateur final tant que les données d'identification de celui-ci peuvent être conservées en vertu de l'article 126 de la loi du 13 juin 2005. Les données à conserver par l'opérateur sont déterminées en fonction de la méthode d'identification choisie, mais comprennent au maximum le nom et le prénom, le sexe, la nationalité, la date et le lieu de naissance, l'adresse du domicile, l'adresse e-mail et le numéro de téléphone, le numéro de registre national, le numéro du document d'identité, le pays d'émission du document lorsqu'il s'agit d'un document étranger et la date de validité du document, les références de l'opération

de paiement, l'association de la carte prépayée au produit pour lequel l'utilisateur final est déjà identifié et la photo de l'utilisateur final, mais uniquement, en ce qui concerne cette dernière, pour les documents autres que la carte d'identité électronique belge. Lorsque la photo se trouvant sur la carte d'identité électronique belge a été transmise à l'opérateur ou au fournisseur d'un service d'identification, ces derniers détruisent cette photo au plus tard avant l'activation de la carte prépayée.

L'arrêté royal du 27 novembre 2016 définit également les méthodes d'identification valides, à savoir l'identification sur la base de documents d'identification en présence de l'utilisateur final (article 14), l'identification en ligne et la signature électronique par la carte d'identité électronique auprès de l'entreprise concernée (article 15), l'identification via le fournisseur d'un service d'identification (article 16), l'identification sur la base de l'opération de paiement en ligne (article 17), l'extension ou la migration de produit (article 18) et la vérification par un moyen de communication électronique (article 19).

B.2.6. Lors des travaux préparatoires, la suppression de l'anonymat des cartes de téléphonie mobile prépayées est justifiée comme suit :

« 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 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 4-6).

B.2.7. Il découle de ce qui précède que l'identifiabilité de tous les utilisateurs finaux de réseaux de communications électroniques constituait dès le départ la prémisse de l'article 127 de la loi du 13 juin 2005 et que l'anonymat des utilisateurs finaux de cartes de téléphonie mobile prépayées a toujours été considéré comme une exception temporaire. En outre, ce n'est pas tant le législateur, mais le Roi qui a supprimé l'anonymat, en prenant l'arrêté royal du 27 novembre 2016.

B.3.1. L'article 16/2 de la loi du 30 novembre 1998, modifié par l'article 3 de la loi attaquée, dispose :

« § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à :

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé;

2° l'identification des services et des moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

La réquisition est effectuée par écrit par le dirigeant de service ou son délégué. En cas d'urgence, le dirigeant de service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite.

Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis donne au dirigeant de service ou à son délégué les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions.

Le dirigeant de service ou son délégué peut, dans le respect des principes de proportionnalité et de subsidiarité, et moyennant l'enregistrement de la consultation, également obtenir les données visées au moyen d'un accès aux fichiers des clients de l'opérateur ou du fournisseur du service. Le Roi fixe, sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, les conditions techniques auxquelles cet accès est possible.

§ 2. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée visée dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d'une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.

La réquisition est effectuée par écrit par le dirigeant de service ou son délégué. En cas d'urgence, le dirigeant de service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite.

Toute banque et toute institution financière qui est requise donne sans délai au dirigeant de service ou à son délégué les données qui ont été demandées.

Les données d'identification que les services de renseignement et de sécurité reçoivent dans le cadre de l'exercice de la méthode visée au présent paragraphe, se limitent aux données d'identification visées au paragraphe 1er.

§ 3. Toute personne qui refuse de communiquer les données ainsi demandées ou de fournir l'accès requis est punie d'une amende de vingt-six euros à dix mille euros.

§ 4. Les services de renseignement et de sécurité tiennent un registre de toutes les identifications requises et de toutes les identifications obtenues par accès direct. Le Comité permanent R reçoit chaque mois du service de renseignement et de sécurité concerné une liste des identifications requises et de tout accès ».

B.3.2. L'identification sur la base de l'opération de paiement en ligne constitue l'une des méthodes d'identification valides visées dans l'arrêté royal du 27 novembre 2016. L'article 17 de cet arrêté royal dispose :

« § 1er. L'entreprise concernée peut identifier l'utilisateur final sur la base d'une opération de paiement électronique en ligne spécifique à l'achat ou la recharge de la carte prépayée.

Cette méthode est soumise aux conditions suivantes :

1° l'opération de paiement doit être traitée par un prestataire de services de paiement tel que visé à l'art. I.9. 2°, *a), b), c),* et *d)* du Code de droit économique;

2° Le prestataire de services de paiement est soumis à la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme;

3° une nouvelle identification doit être effectuée dans les 18 mois qui suivent l'opération de paiement liée à la carte prépayée;

4° l'utilisateur final introduit sur un formulaire en ligne de l'entreprise concernée au minimum son nom, son prénom et le lieu et la date de sa naissance.

§ 2. L'entreprise concernée conserve la référence de l'opération de paiement et les données du formulaire en ligne ».

B.3.3. Lors des travaux préparatoires, le concours que doivent prêter les banques ou les institutions financières a été justifiée comme suit :

« 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 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 14-16).

Quant au premier moyen

B.4. Les parties requérantes prennent un premier moyen de la violation, par l'article 2 de la loi attaquée, des articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne (ci-après : la Charte) et avec les articles 2, point *a)*, et 6 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », en ce que cette disposition conférerait au Roi une habilitation trop large et insuffisamment précise pour fixer le contenu de l'obligation d'identification attaquée.

B.5.1. Le principe d'égalité et de non-discrimination n'exclut pas qu'une différence de traitement soit établie entre des catégories de personnes, pour autant qu'elle repose sur un critère objectif et qu'elle soit raisonnablement justifiée.

L'existence d'une telle justification doit s'apprécier en tenant compte du but et des effets de la mesure critiquée ainsi que de la nature des principes en cause; le principe d'égalité et de non-discrimination est violé lorsqu'il est établi qu'il n'existe pas de rapport raisonnable de proportionnalité entre les moyens employés et le but visé.

B.5.2. L'article 22 de la Constitution dispose :

« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ».

L'article 8 de la Convention européenne des droits de l'homme dispose :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

L'article 7 de la Charte dispose :

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

L'article 8 de la Charte dispose :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

L'article 52, paragraphe 1, de la Charte dispose :

« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

L'article 52, paragraphe 3, de la Charte dispose :

« Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue ».

B.5.3. Le Constituant a recherché la plus grande concordance possible entre l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme (*Doc. parl.*, Chambre, 1992-1993, nº 997/5, p. 2).

La portée de cet article 8 est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un tout indissociable.

Lorsque la Charte contient des droits correspondant à des droits garantis par la Convention européenne des droits de l'homme, « leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ». Cette disposition aligne le sens et la portée des droits qui sont garantis par la Charte sur les droits correspondants qui sont garantis par la Convention européenne des droits de l'homme.

Les explications relatives à la Charte (2007/C 303/02), publiées au *Journal officiel* du 14 décembre 2007, indiquent que, parmi les articles « dont le sens et la portée sont les mêmes que ceux des articles correspondants dans la CEDH », l'article 7 de la Charte correspond à l'article 8 de la Convention européenne des droits de l'homme.

La Cour de justice de l'Union européenne rappelle à cet égard que « l'article 7 de la Charte, relatif au droit au respect de la vie privée et familiale, contient des droits correspondant à ceux garantis par l'article 8, paragraphe 1, de la [Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après : la CEDH),] et qu'il convient donc, conformément à l'article 52, paragraphe 3, de la Charte, de donner audit article 7 le même sens et la même portée que ceux conférés à l'article 8, paragraphe 1, de la CEDH, tel qu'interprété par la jurisprudence de la Cour européenne des droits de l'homme » (CJUE, 17 décembre 2015, C-419/14, *WebMindLicenses Kft.*, point 70; 14 février 2019, C-345/17, *Buivids*, point 65).

En ce qui concerne l'article 8 de la Charte, la Cour de justice considère qu'« ainsi que le prévoit expressément l'article 52, paragraphe 3, seconde phrase, de la Charte, l'article 52, paragraphe 3, première phrase, de celle-ci ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue que la CEDH », et que « l'article 8 de la Charte concerne un droit fondamental distinct de celui consacré à l'article 7 de celle-ci et qui n'a pas d'équivalent dans la CEDH » (CJUE, grande chambre, 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige*, point 129).

Il découle de ce qui précède que, dans le champ d'application du droit de l'Union européenne, l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme et l'article 7 de la Charte garantissent des droits fondamentaux analogues, alors que l'article 8 de cette Charte vise spécifiquement la protection des données à caractère personnel.

B.5.4. En vertu de l'article 94, paragraphe 1, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) » (ci-après : le RGPD), la directive 95/46/CE est abrogée avec effet au 25 mai 2018.

L'article 5 du RGPD, qui a reproduit *mutatis mutandis* le contenu de l'article 6 de la directive 95/46/CE, dispose :

« 1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

B.6. En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout justiciable qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

Une délégation au pouvoir exécutif n'est toutefois pas contraire au principe de la légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur.

B.7.1. Selon le Conseil des ministres, le moyen est irrecevable, étant donné que la disposition attaquée comporte seulement une nouvelle délégation au Roi, plus précisément la délégation qui a été insérée dans le nouvel article 127, § 3, alinéa 2, de la loi du 13 juin 2005 et qui n'est pas attaquée par les parties requérantes. Les autres délégations au Roi étaient déjà contenues dans l'article 127 de cette loi avant l'entrée en vigueur de la disposition attaquée.

B.7.2. Un recours dirigé contre une différence de traitement ne résultant pas de la loi attaquée mais déjà contenue dans une loi antérieure est irrecevable.

Toutefois, lorsque, dans une législation nouvelle, le législateur reprend une disposition ancienne et s'approprie de cette manière son contenu, un recours peut être introduit contre la disposition reprise, dans les six mois de sa publication.

B.7.3. La disposition attaquée a modifié l'article 127 de la loi du 13 juin 2005 sur différents points, même si, à cette occasion, comme il est dit en B.2.7, le législateur est resté fidèle à la prémisse initiale de l'identifiabilité de tous les utilisateurs finaux de réseaux de communications électroniques. En édictant la disposition attaquée, il s'est donc approprié le contenu de l'article 127 de la loi du 13 juin 2005.

L'exception est rejetée.

B.8.1. La Commission de la protection de la vie privée (actuellement l'Autorité de protection des données) a formulé, dans un avis relatif à l'avant-projet ayant donné lieu à la loi attaquée, quelques observations concernant le respect du principe de la légalité en matière de restrictions du droit au respect de la vie privée :

« 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) » (CPVP, avis nº 54/2015, 15 décembre 2015, *Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 38-42).

La section de législation du Conseil d'État a elle aussi formulé, dans son avis relatif à cet avant-projet, quelques observations sur le respect du principe de la légalité en matière de restrictions du droit au respect de la vie privée :

« 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 » (Conseil d'État, section de législation, avis nº 59.423/4, 15 juin 2016, *Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 47-48).

B.8.2. Le législateur n'a que partiellement suivi ces avis. Il a notamment choisi, en dépit de ceux-ci, de ne pas indiquer dans la disposition attaquée les données d'identification qui peuvent être collectées et traitées et les documents d'identification qui entrent en considération. Ce choix a été justifié lors des travaux préparatoires comme suit :

« 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 nº 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 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 6-7).

B.8.3.1. L'article 127 de la loi du 13 juin 2005 règle lui-même le principe de l'identifiabilité de l'utilisateur final tant des anciennes cartes prépayées que des nouvelles. Il lie la suppression de l'anonymat des cartes prépayées à la date à laquelle l'arrêté d'exécution entre en vigueur et y ajoute qu'il est interdit, à partir de cette date, de fournir des services ou des équipements susceptibles de rendre l'identification difficile. Il dispose aussi que, sauf preuve contraire, l'utilisateur final identifié est présumé utiliser lui-même le service de communications électroniques.

Il mentionne également les catégories de personnes à qui sont imposées des obligations dans ce contexte, à savoir les opérateurs, les fournisseurs, les canaux de vente, les entreprises qui fournissent un service d'identification et les utilisateurs finaux. Il définit enfin le but de l'identifiabilité, à savoir le bon fonctionnement des services d'urgence, l'enquête pénale et le fonctionnement des services de renseignement et de sécurité.

B.8.3.2. Sur le plan de l'identifiabilité, l'article 127 de la loi du 13 juin 2005 confère plusieurs habilitations au Roi. Tout d'abord, il L'habilite à fixer, de manière générale, les mesures techniques et administratives qui doivent être imposées dans ce contexte aux parties concernées. Il doit également déterminer qui sont les utilisateurs finaux non identifiés de cartes prépayées achetées avant l'entrée en vigueur de l'arrêté d'exécution. Il doit aussi fixer le délai maximal dans lequel les utilisateurs finaux non identifiés doivent s'identifier auprès de leur opérateur, même si l'article 127 de la loi du 13 juin 2005 limite cette habilitation en disposant que ce délai ne peut pas excéder six mois. Enfin, le Roi doit déterminer les tarifs rétribuant le concours des opérateurs et des fournisseurs à l'identification d'un utilisateur final.

Ces habilitations portent sur l'exécution de mesures dont les éléments essentiels ont été préalablement déterminés par le législateur.

B.8.4.1. Pour ce qui est des données d'identification et des documents d'identification concernés, l'article 127 de la loi attaquée dispose qu'il doit s'agir de documents comportant le numéro de registre national et que le numéro de registre national est une donnée à caractère personnel qui doit être collectée et traitée dans ce contexte. Les autres données d'identification, ainsi que les documents d'identification qui entrent en considération, ne sont pas énumérés dans cette disposition législative, en dépit des avis mentionnés en B.8.1.

B.8.4.2. En outre, le législateur n'a pas donné au Roi une habilitation explicite pour définir plus précisément ces données d'identification et ces documents d'identification. De tels éléments essentiels d'un traitement de données à caractère personnel ne sauraient toutefois être couverts par l'habilitation vague conférée par l'article 127, § 1er, alinéa 1er, de la loi du 13 juin 2005 et qui consiste à prendre les « mesures techniques et administratives » nécessaires en vue de l'identifiabilité de l'utilisateur final.

Le Roi devait dès lors déterminer ces données et ces documents d'identification sur la base du pouvoir qu'Il tire de l'article 108 de la Constitution de faire les règlements et les arrêtés nécessaires pour l'exécution des lois.

Toutefois, ce pouvoir général d'exécution du Roi ne saurait suffire en l'espèce. En effet, la délégation d'éléments essentiels d'une matière réservée par le Constituant au pouvoir législatif n'est possible que si le respect de la procédure parlementaire ne permet pas au législateur de réaliser un objectif d'intérêt général et à condition qu'il détermine explicitement et sans équivoque l'objet de cette habilitation et que les mesures prises par le Roi soient examinées par le pouvoir législatif, en vue de leur confirmation, dans un délai relativement court, fixé dans la loi d'habilitation.

B.8.4.3. Lors des travaux préparatoires, le législateur justifie cette méthode de travail par le caractère technique des données d'identification et des documents d'identification, la nécessité de pouvoir en adapter l'énumération en fonction de nouveaux enseignements et le fait que, dans le cadre de la conservation des données, ces données n'étaient pas non plus énumérées dans l'article 126 de la loi du 13 juin 2005 lui-même annulé par l'arrêt de la Cour nº 57/2021 du 22 avril 2021.

Indépendamment du fait que ces arguments ne sauraient expliquer l'absence d'une habilitation explicite et sans équivoque, le caractère technique des données d'identification et des documents d'identification et l'adaptabilité d'une telle énumération ne suffisent pas pour conclure que le fait d'ancrer de tels éléments dans une norme législative ne permettrait pas au législateur de réaliser un objectif d'intérêt général. En effet, même une norme législative peut être modifiée. Le Conseil des ministres ne démontre pas qu'une modification de ces données d'identification peut être urgente au point de ne pas pouvoir suivre le cours normal de la procédure législative. De même, une énumération des données d'identification et des documents d'identification n'est pas complexe au point de ne pas pouvoir être inscrite dans une norme législative. Enfin, le législateur ne saurait justifier une violation de la Constitution en renvoyant à une autre disposition législative qui comportait peut-être la même inconstitutionnalité.

B.8.4.4. Au demeurant, l'article 127 de la loi du 13 juin 2005 délimite insuffisamment le pouvoir d'exécution du Roi pour déterminer les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération. En ce qui concerne les documents d'identification, il mentionne seulement qu'il doit s'agir de documents comprenant le numéro de registre national. En ce qui concerne les données d'identification autres que le numéro de registre national, il ne comporte pas la moindre précision.

B.8.5. Pour ce qui est de la collecte et du traitement des données et des documents d'identification, l'article 127 de la loi du 13 juin 2005 définit qui collecte les données, à savoir le canal de vente ou l'entreprise qui offre un service d'identification. Il dispose également que le canal de vente ne peut pas conserver ces données et ces documents et qu'il doit les détruire au plus tard au moment de l'activation de la carte de téléphonie mobile prépayée.

En ce qui concerne le mode de traitement des données, l'article 127 de la loi du 13 juin 2005 définit qui est le responsable du traitement, à savoir l'opérateur ou le fournisseur. Il dispose également que le canal de vente transmet les données collectées à l'opérateur, au fournisseur ou à l'entreprise qui offre un service d'identification, par une introduction directe dans un système informatique ou à l'aide d'une copie du document d'identification. Il dispose également que l'opérateur et le fournisseur doivent conserver une copie de tout document d'identification autre que la carte d'identité électronique belge et que les données d'identification traitées doivent être conservées conformément à l'article 126, § 3, de la loi du 13 juin 2005.

B.8.6. En ce qui concerne les sanctions, l'article 127, §§ 4 et 5, de la loi du 13 juin 2005 dispose que les opérateurs ou les fournisseurs qui ne respectent pas les mesures techniques et administratives imposées par le Roi ne peuvent plus fournir le service pour lequel ces mesures n'ont pas été prises. Il dispose également que les utilisateurs finaux qui ne respectent pas les obligations qui leur incombent doivent être déconnectés, sans indemnité, du réseau de communications électroniques.

B.8.7.1. Les parties requérantes reprochent en outre à la disposition attaquée de ne pas fixer des critères distincts pour les utilisateurs finaux d'anciennes et de nouvelles cartes prépayées.

L'article 127 de la loi du 13 juin 2005, tel qu'il a été modifié par l'article 2 de la loi attaquée, soumet toutefois les deux catégories d'utilisateurs finaux de manière égale à l'obligation d'identifiabilité. À cet égard, l'article 127, § 3, alinéa 2, de cette loi fixe un délai maximal dans lequel les utilisateurs finaux d'anciennes cartes prépayées doivent satisfaire aux mesures administratives et techniques fixées par le Roi, alors que la nouvelle réglementation était applicable aux nouvelles cartes prépayées dès son entrée en vigueur.

B.8.7.2. En ce que les parties requérantes reprochent à la disposition attaquée de ne pas préciser suffisamment clairement les catégories d'utilisateurs finaux de réseaux de communications électroniques auxquelles elle s'applique, il suffit de constater que, conformément à l'objectif initial de l'article 127 de la loi du 13 juin 2005, tous les utilisateurs finaux relèvent de son champ d'application, indépendamment du fait qu'ils disposent d'un abonnement ou d'une carte de téléphonie mobile prépayée. Comme il est dit en B.2.6, l'assimilation des utilisateurs finaux d'une carte de téléphonie mobile prépayée aux titulaires d'abonnements constitue d'ailleurs l'un des objectifs de la loi attaquée.

B.8.7.3. En ce que les parties requérantes reprochent à la disposition attaquée de ne pas préciser les circonstances du traitement des données, il y a lieu de constater que cette disposition renvoie à cet égard à l'article 126, § 3, de la loi du 13 juin 2005.

Par son arrêt nº 57/2021 du 22 avril 2021, la Cour a annulé notamment l'article 4 de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques ». Par son arrêt nº 84/2015 du 11 juin 2015, la Cour avait déjà annulé la loi du 30 juillet 2013 « portant modification des articles 2, 126

et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle ». À la suite de ces arrêts, l'article 126 de la loi du 13 juin 2005 est actuellement applicable dans la version qui a été modifiée pour la dernière fois par l'article 33 de la loi du 4 février 2010 « relative aux méthodes de recueil des données par les services de renseignement et de sécurité ». Les annulations mentionnées reposaient en substance sur l'interdiction d'une conservation généralisée et indifférenciée des données. Cette interdiction trouvant son fondement dans le droit de l'Union, l'article 126 de la loi du 13 juin 2005 ne saurait être réputé applicable dans la version qui précède ces annulations, en ce que celle-ci porte sur une conservation généralisée et indifférenciée des données en matière de communications électroniques. La même disposition peut cependant être applicable en ce qu'elle porte sur les données d'identification des utilisateurs de cartes de téléphonie mobile prépayées visées à l'article 127 de la même loi. L'article 126, tel qu'il a été modifié par la loi du 4 février 2010, dispose :

« § 1er. Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

§ 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut.

Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique ».

En exécution de cette disposition, l'arrêté royal du 19 septembre 2013 « portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques » (ci-après : l'arrêté royal du 19 septembre 2013) règle actuellement le traitement et la conservation des données à caractère personnel, y compris en ce qui concerne les données d'identification qui sont collectées sur la base de l'article 127 de la loi du 13 juin 2005.

Dans son mémoire complémentaire et lors de l'audience, le Conseil des ministres a d'ailleurs souligné qu'une nouvelle version de l'article 126 de la loi du 13 juin 2005 est en préparation, pour satisfaire aux exigences de l'arrêt de la Cour nº 57/2021 et de la jurisprudence de la Cour de justice de l'Union européenne qui y est appliquée.

B.8.7.4. En ce que les parties requérantes reprochent à la disposition attaquée de ne pas déterminer qui a accès aux données d'identification conservées ni les conditions de cet accès, il suffit de constater que cet accès n'est pas réglé par l'article 127 de la loi du 13 juin 2005, mais par les articles 46*bis*, 88*bis* et 90*ter* à 90*decies* du Code d'instruction criminelle en ce qui concerne l'accès dans le cadre d'une instruction pénale, par l'article 16/2, § 1er, de la loi du 30 novembre 1998 en ce qui concerne l'accès par les services de renseignement et de sécurité et par l'article 107, § 2, de la loi du 13 juin 2005 en ce qui concerne l'accès par les services d'urgence.

B.8.8. En outre, en accordant une telle délégation, le législateur ne pouvait habiliter le Roi à prendre des dispositions qui entraîneraient une violation du droit au respect de la vie privée. Il appartient au juge compétent de vérifier si le Roi a fait un usage légal ou non de la délégation qui Lui est accordée.

B.9.1. Il ressort de ce qui précède que l'article 127 de la loi du 13 juin 2005, tel qu'il a été modifié par l'article 2 de la loi attaquée, viole le principe de légalité garanti par l'article 22 de la Constitution, mais seulement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération. Dans cette mesure, il y a lieu d'annuler l'article 2 de la loi attaquée.

Pour le surplus, le premier moyen n'est pas fondé, étant donné que les habilitations conférées au Roi et qui sont attaquées portent sur l'exécution de mesures dont les éléments essentiels ont été fixés au préalable par le législateur.

B.9.2. Contrairement à ce que les parties requérantes font valoir, la Cour européenne des droits de l'homme n'a pas jugé, par son arrêt *Rotaru*, que le traitement des données à caractère personnel et l'accès aux données traitées doivent être réglés par le pouvoir législatif. Elle a seulement souligné que ce traitement et cet accès doivent avoir une base claire, accessible et prévisible dans la réglementation interne (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, §§ 47-63).

La Cour de justice aussi exige seulement que « la base légale qui permet l'ingérence dans [le droit au respect de la vie privée] doit définir elle-même la portée de la limitation de l'exercice du droit concerné » (CJUE, 6 octobre 2020, C-623/17, *Privacy international*, point 65). Elle n'exige pas que tous les aspects de cette limitation soient réglés par une loi formelle.

Un contrôle de la disposition attaquée au regard de l'article 8 de la Convention européenne des droits de l'homme, des articles 7 et 8 de la Charte ou de l'article 5 du RGPD ne conduit dès lors pas à une autre conclusion, étant donné que ces dispositions ne permettent pas de déduire des exigences plus strictes en ce qui concerne le principe de la légalité formelle que celles qui découlent de l'article 22 de la Constitution.

B.9.3. Étant donné que la violation constatée porte uniquement sur l'article 22 de la Constitution et non sur les normes du droit de l'Union européenne invoquées dans le moyen, il appartient à la Cour, en vertu de l'article 8, alinéa 3, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, d'indiquer ceux des effets des dispositions annulées qui doivent être considérés comme définitifs ou maintenus provisoirement pour le délai qu'elle détermine.

La violation constatée de l'article 22 de la Constitution ne porte pas sur la nature et le contenu des données d'identification ou des documents d'identification tels qu'ils sont actuellement réglés dans l'arrêté royal du 27 novembre 2016 et tels qu'ils échappent au pouvoir de contrôle de la Cour. Elle porte uniquement sur le fait que ces données et documents doivent être énumérés dans une disposition législative.

Il y a donc lieu de donner au législateur le temps nécessaire pour prévoir ce fondement légal, sans qu'il faille dans l'intervalle annuler l'identification des utilisateurs finaux de cartes de téléphonie mobile prépayées réglée par la disposition attaquée. En outre, ce délai doit être suffisamment long pour permettre au législateur d'aligner ce fondement légal sur la nouvelle réglementation en matière de conservation des données qui est en préparation, à la suite de l'arrêt de la Cour nº 57/2021 du 22 avril 2021.

Par conséquent, il y a lieu de maintenir les effets de la disposition attaquée comme il est indiqué dans le dispositif.

Quant au deuxième moyen

B.10. Les parties requérantes prennent un deuxième moyen de la violation, par les articles 2 et 3 de la loi attaquée, des articles 10, 11, 19, 22 et 25 de la Constitution, lus en combinaison avec les articles 8 et 10 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11 et 52 de la Charte, avec les articles 56 et 57 du Traité sur le fonctionnement de l'Union européenne, avec les articles 2, point *a)*, et 6 de la directive 95/46/CE et avec les articles 1er, 2, 3, 5, 6, 9 et 15 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ». Ce moyen se subdivise en trois branches.

B.11.1. L'article 19 de la Constitution dispose :

« La liberté des cultes, celle de leur exercice public, ainsi que la liberté de manifester ses opinions en toute matière, sont garanties, sauf la répression des délits commis à l'occasion de l'usage de ces libertés ».

L'article 25 de la Constitution dispose :

« La presse est libre; la censure ne pourra jamais être établie; il ne peut être exigé de cautionnement des écrivains, éditeurs ou imprimeurs.

Lorsque l'auteur est connu et domicilié en Belgique, l'éditeur, l'imprimeur ou le distributeur ne peut être poursuivi ».

L'article 10 de la Convention européenne des droits de l'homme dispose :

« 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.

2. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ».

L'article 11 de la Charte dispose :

« 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.

2. La liberté des médias et leur pluralisme sont respectés ».

En ce qu'ils reconnaissent le droit à la liberté d'expression, l'article 10 de la Convention européenne des droits de l'homme et l'article 11, paragraphe 1, de la Charte ont une portée analogue à celle de l'article 19 de la Constitution, qui reconnaît la liberté de manifester ses opinions en toute matière.

Dès lors, les garanties fournies par ces dispositions forment, dans cette mesure, un ensemble indissociable.

B.11.2. L'article 56 du Traité sur le fonctionnement de l'Union européenne dispose :

« Dans le cadre des dispositions ci-après, les restrictions à la libre prestation des services à l'intérieur de l'Union sont interdites à l'égard des ressortissants des États membres établis dans un État membre autre que celui du destinataire de la prestation.

Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, peuvent étendre le bénéfice des dispositions du présent chapitre aux prestataires de services ressortissants d'un État tiers et établis à l'intérieur de l'Union ».

L'article 57 du Traité sur le fonctionnement de l'Union européenne dispose :

« Au sens des traités, sont considérées comme services les prestations fournies normalement contre rémunération, dans la mesure où elles ne sont pas régies par les dispositions relatives à la libre circulation des marchandises, des capitaux et des personnes.

Les services comprennent notamment :

a) des activités de caractère industriel,

b) des activités de caractère commercial,

c) des activités artisanales,

d) les activités des professions libérales.

Sans préjudice des dispositions du chapitre relatif au droit d'établissement, le prestataire peut, pour l'exécution de sa prestation, exercer, à titre temporaire, son activité dans l'État membre où la prestation est fournie, dans les mêmes conditions que celles que cet État impose à ses propres ressortissants ».

B.11.3. Les articles 1er, 2, 3, 5, 6, 9 et 15 de la directive 2002/58/CE disposent :

« Article premier. Champ d'application et objectif

1. La présente directive prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté.

2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal.

Article 2. Définitions

Sauf disposition contraire, les définitions figurant dans la directive 95/46/CE et dans la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive ' cadre ') s'appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables :

a) ' utilisateur ' : toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service;

b) ' données relatives au trafic ' : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation;

c) ' données de localisation ' : toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;

d) ' communication ' : toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit;

f) le ' consentement ' d'un utilisateur ou d'un abonné correspond au ' consentement de la personne concernée ' figurant dans la directive 95/46/CE;

g) ' service à valeur ajoutée ' : tout service qui exige le traitement de données relatives au trafic ou à la localisation, à l'exclusion des données qui ne sont pas indispensables pour la transmission d'une communication ou sa facturation;

h) ' courrier électronique ' : tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère.

i) ' violation de données à caractère personnel ' : une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté.

Article 3. Services concernés

1. La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans la Communauté, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification.

[...]

Article 5. Confidentialité des communications

1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.

2. Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale.

3. Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur, ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

Article 6. Données relatives au trafic

1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1.

2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

3. Afin de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d'un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1 dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services, pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.

4. Le fournisseur de service doit informer l'abonné ou l'utilisateur des types de données relatives au trafic qui sont traités ainsi que de la durée de ce traitement aux fins visées au paragraphe 2 et, avant d'obtenir leur consentement, aux fins visées au paragraphe 3.

5. Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées d'assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée; ce traitement doit se limiter à ce qui est nécessaire à de telles activités.

6. Les paragraphes 1, 2, 3 et 5 s'appliquent sans préjudice de la possibilité qu'ont les organes compétents de se faire communiquer des données relatives au trafic conformément à la législation en vigueur dans le but de régler des litiges, notamment en matière d'interconnexion ou de facturation.

[...]

Article 9. Données de localisation autres que les données relatives au trafic

1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic.

2. Lorsque les utilisateurs ou les abonnés ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic, ils doivent garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

3. Le traitement des données de localisation autres que les données relatives au trafic effectué conformément aux paragraphes 1 et 2 doit être restreint aux personnes agissant sous l'autorité du fournisseur du réseau public de communications ou service de communications électroniques accessible au public ou du tiers qui fournit le service à valeur ajoutée, et doit se limiter à ce qui est nécessaire pour assurer la fourniture du service à valeur ajoutée.

[...]

Article 15. Application de certaines dispositions de la directive 95/46/CE

1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

1*bis*. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication aux fins visées à l'article 1er, paragraphe 1, de ladite directive.

1*ter*. Les fournisseurs établissent, sur la base des dispositions nationales adoptées au titre du paragraphe 1, des procédures internes permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Ils mettent, sur demande, à la disposition de l'autorité nationale compétente des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur leur réponse.

2. Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

3. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électroniques ».

En ce qui concerne la première branche du deuxième moyen

B.12. Dans la première branche du deuxième moyen, les parties requérantes font valoir que l'obligation d'identification généralisée et indifférenciée imposée par la loi attaquée à tous les utilisateurs finaux de services de communications électroniques constitue une ingérence dans le droit au respect de la vie privée qui va au-delà de ce qui est nécessaire au regard des objectifs poursuivis.

B.13.1. Le droit au respect de la vie privée n'est pas absolu. Les dispositions constitutionnelles et conventionnelles n'excluent pas une ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée, mais exigent que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit.

Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée : pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait ménagé un juste équilibre entre tous les droits et intérêts en cause. Pour juger de cet équilibre, la Cour européenne des droits de l'homme tient compte notamment des dispositions de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de la recommandation nº R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (CEDH, 25 février 1997, *Z c. Finlande*, § 95; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 103).

B.13.2. Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient de tenir compte notamment de leur caractère automatisé, des techniques utilisées, de la précision, de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de droits de contrôle et de voies de recours suffisants pour les personnes concernées, de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont traitées, du caractère distinctif de la réglementation et de la présence ou de l'absence de garanties visant à éviter l'usage inapproprié et abusif, par les services publics, des données à caractère personnel traitées (arrêt nº 108/2016 du 14 juillet 2016, B.12.2; arrêt nº 29/2018 du 15 mars 2018, B.14.4; arrêt nº 27/2020 du 20 février 2020, B.8.3; CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, § 59; décision, 29 juin 2006, *Weber et Saravia c. Allemagne*, § 135; 28 avril 2009, *K.H. e.a. c. Slovaquie*, §§ 60-69; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, §§ 101-103, 119, 122 et 124; 18 avril 2013, *M.K. c. France*, §§ 37 et 42-44; 18 septembre 2014, *Brunet c. France*, §§ 35-37; 12 janvier 2016, *Szabó et Vissy c. Hongrie*, § 68; 30 janvier 2020, *Breyer c. Allemagne*, §§ 73-80; grande chambre, 25 mai 2021, *Centrum för rättvisa c. Suède*, §§ 262-278; grande chambre, 25 mai 2021, *Big Brother Watch c. Royaume-Uni*, §§ 348-364; CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, et C-594/12, *Kärntner Landesregierung e.a.*, points 56-66; grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, points 105-133; grande chambre, 6 octobre 2020, C-623/17, *Privacy International*, points 58-82; grande chambre, 2 mars 2021, C-746/18, *Prokuratuur*, points 50-56).

B.13.3. Il ressort de la jurisprudence de la Cour européenne des droits de l'homme que les données à caractère personnel ne peuvent pas être conservées plus longtemps que nécessaire pour la réalisation de la finalité pour laquelle elles ont été enregistrées sous une forme qui permette l'identification ou qui permette d'établir un lien entre une personne et des faits infractionnels. Pour apprécier la proportionnalité de la durée de conservation par rapport à l'objectif pour lequel les données ont été enregistrées, la Cour européenne des droits de l'homme tient compte de l'existence ou non d'un contrôle indépendant concernant la justification de la conservation des données dans les banques de données sur la base de critères précis, tels que la gravité des faits, le fait que la personne concernée a déjà fait l'objet dans le passé d'une arrestation, la force des soupçons qui pèsent sur une personne et toute autre circonstance particulière (CEDH, grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 103; 18 avril 2013, *M.K. c. France*, § 35; 17 décembre 2009, *B.B. c. France*, § 61; 18 septembre 2014, *Brunet c. France*, §§ 35-40).

B.14.1. En ce qui concerne la collecte, le traitement et la conservation généralisés et indifférenciés de données à caractère personnel des utilisateurs de réseaux de communication électroniques, tant la Cour européenne des droits de l'homme que la Cour de justice font une distinction entre, d'une part, les données relatives au trafic et les données de localisation et, d'autre part, les données d'identification.

B.14.2. Elles considèrent la collecte, le traitement et la conservation de données relatives au trafic et de données de localisation de ces utilisateurs comme une très grave limitation du droit au respect de la vie privée, puisque de telles données sont susceptibles de révéler des informations sensibles sur un nombre important d'aspects de la vie privée des personnes concernées, comme leur orientation sexuelle, leurs opinions politiques, leurs convictions religieuses, philosophiques, sociétales ou autres et leur état de santé.

De telles données peuvent permettre de tirer des conclusions très précises sur la vie privée des personnes dont les données sont conservées, telles que leurs habitudes quotidiennes, leurs lieux de séjour permanents ou temporaires, leurs déplacements journaliers ou autres, leurs activités, leurs relations sociales et les milieux sociaux qu'elles fréquentent. Ces données fournissent les moyens d'établir un profil des personnes concernées, information tout aussi sensible que le contenu même de la communication (CEDH, grande chambre, 25 mai 2021, *Centrum för rättvisa c. Suède*, §§ 238-245; grande chambre, 25 mai 2021, *Big Brother Watch c. Royaume-Uni*, § 324-331; CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 117; grande chambre, 6 octobre 2020, C-623/17, *Privacy International*, point 71).

La Cour de justice en déduit que la collecte, le traitement et la conservation généralisés et indifférenciés de données relatives au trafic et de données de localisation sont en principe interdits. Ils ne sont autorisés que pour des raisons de sécurité nationale et uniquement dans la mesure où il existe suffisamment d'indices concrets que l'État membre concerné fait face à une menace grave pour la sécurité nationale et que cette menace est réelle, actuelle et prévisible. En outre, cette conservation ne peut pas durer plus longtemps que strictement nécessaire par rapport à cette menace pour la sécurité nationale et doit être assortie de garanties strictes permettant de protéger efficacement les données à caractère personnel contre les risques d'abus, notamment à l'aide d'un contrôle effectif exercé par une juridiction ou par une entité administrative indépendante (CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, points 137-139). En revanche, une collecte, un traitement et une conservation de données relatives au trafic et de données de localisation en vue de lutter contre la criminalité grave ne peuvent pas avoir un caractère généralisé et indifférencié, mais doivent être délimités sur la base de critères géographiques ou liés à certaines personnes (*ibid.*, points 144-150).

Par contre, la Cour européenne des droits de l'homme n'interdit pas la collecte, le traitement et la conservation généralisés et indifférenciés de données relatives au trafic et de données de localisation, mais les soumet à un contrôle strict. Elle apprécie la légalité et la nécessité de telles mesures dans une société démocratique au regard des motifs pour lesquels l'interception en masse est ordonnée, des circonstances dans lesquelles les communications de personnes privées sont interceptées, de la procédure d'octroi d'une autorisation d'interception en masse, de la procédure à suivre pour la sélection du matériel à utiliser, des précautions qui sont prises si les données traitées sont communiquées à des tiers, des limites posées à la durée de l'interception et de la conservation des données à caractère personnel, en ce compris les circonstances dans lesquelles les données sont détruites, de la procédure et des modalités de contrôle *a priori* exercé par une autorité indépendante quant au respect des garanties, en ce compris la réparation ordonnée par cette autorité, et de la procédure de contrôle indépendant effectué *a posteriori* quant au respect de toutes les règles applicables (CEDH, grande chambre, 25 mai 2021, *Centrum för rättvisa c. Suède*, § 275; grande chambre, 25 mai 2021, *Big Brother Watch c. Royaume Uni*, § 361).

B.14.3. En revanche, la Cour européenne des droits de l'homme et la Cour de justice considèrent la collecte, le traitement et la conservation généralisés et indifférenciés de simples données d'identification d'utilisateurs de réseaux de communications électroniques comme une limitation moins grave du droit au respect de la vie privée, parce que ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires d'une communication, ni l'endroit où cette communication a eu lieu ou la fréquence de communication avec certaines personnes pendant une période donnée. Ces données ne fournissent donc aucune information sur les communications données par ces personnes ni sur leur vie privée. Ces seules données ne permettent pas d'établir un profil de l'utilisateur ni de suivre ses mouvements (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, §§ 92-95; CJUE, 2 octobre 2018, C-207/16, *Ministerio Fiscal*, point 62; grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 157).

La Cour de justice en déduit que le droit au respect de la vie privée ne s'oppose pas à une collecte, à un traitement et à une conservation généralisés et indifférenciés de données d'identification d'utilisateurs de réseaux de communications électroniques aux fins de la recherche, de la détection et de la poursuite d'infractions pénales ainsi que de la sauvegarde de la sécurité publique. À cet égard, il n'est pas nécessaire qu'il s'agisse d'infractions pénales graves ni de menaces ou d'atteintes graves à la sécurité publique (CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 159). Par contre, il y a lieu de démontrer que « ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus » (*ibid.*, point 168).

La Cour européenne des droits de l'homme contrôle la collecte, le traitement et la conservation généralisés et indifférenciés de ces données d'identification de manière moins intensive que la collecte, le traitement et la conservation de données relatives au trafic et de données de localisation. Elle vérifie tout d'abord si le délai de conservation est raisonnable, compte tenu de la durée habituelle d'une enquête pénale. En ce qui concerne l'accès aux données d'identification conservées, elle exige que les autorités qui peuvent consulter les données soient limitativement énumérées dans la réglementation applicable, que leur accès soit basé sur un fondement légal spécifique et clair dans le droit de la procédure pénale ou dans la législation relative aux services de renseignement et de sécurité et qu'elle soit justifiée par une suspicion concrète initiale. Dès que l'autorité n'a plus besoin des données d'identification demandées, elle doit les détruire immédiatement. La Cour européenne des droits de l'homme n'exige pas que l'intéressé soit informé de l'accès à ses données d'identification. Elle n'exige pas non plus qu'une supervision *a priori* soit organisée accéder à de simples données d'identification : un accès *a posteriori* à une instance judiciaire ou administrative indépendante, combiné aux recours de droit commun dont le prévenu dispose au cours d'un procès pénal, suffit (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, §§ 96-107).

B.15.1. Par son arrêt n° 57/2021 du 22 avril 2021, la Cour a annulé les articles 2, *b)*, 3 à 11 et 14 de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques » au motif qu'ils réglaient une collecte, un traitement et une conservation généralisés et indifférenciés tant de données d'identification que de données relatives au trafic et de données de localisation. La Cour a constaté que « la loi attaquée [reposait], dans son principe même, sur une obligation de conservation généralisée et indifférenciée de l'ensemble des données visées à l'article 126, § 3, de la loi du 13 juin 2005, et qu'elle [poursuivait], d'une manière générale, [...] des objectifs plus larges que la lutte contre la criminalité grave ou le risque d'atteinte à la sécurité publique » (B.17). En outre, la loi attaquée ne garantissait pas que la collecte, le traitement et la conservation de données relatives aux communications électroniques constituaient l'exception et non la règle, ni que l'accès à ces données était soumis à des règles claires et précises, que l'ingérence dans le droit au respect de la vie privée se limitait au strict nécessaire et que chaque ingérence répondait à des critères objectifs, établissant un rapport entre les données à conserver et le but poursuivi (B.18).

B.15.2. La loi présentement attaquée, en revanche, porte uniquement sur les données visées à l'article 127 de la loi du 13 juin 2005, à l'aide desquelles l'utilisateur final d'un service de communications électroniques fourni sur la base d'une carte de téléphonie mobile prépayée peut être identifié. L'article 12, alinéa 2, de l'arrêté royal du 27 novembre 2016 dispose que ces données d'identification peuvent varier en fonction de la méthode d'identification choisie, mais il énumère par la même occasion limitativement les données d'identification que l'entreprise concernée peut conserver au maximum :

« 1° le nom et le prénom;

2° le sexe;

3° la nationalité;

4° la date et le lieu de naissance;

5° l'adresse du domicile, l'adresse e-mail et le numéro de téléphone;

6° le numéro de registre national;

7° le numéro du document d'identité, le pays d'émission du document lorsqu'il s'agit d'un document étranger et la date de validité du document;

8° les références de l'opération de paiement conformément à l'article 17;

9° l'association de la carte prépayée au produit pour lequel l'utilisateur final est déjà identifié conformément à l'article 18;

10° la photo de l'utilisateur final, mais uniquement pour les documents autres que la carte d'identité électronique belge ».

Compte tenu de l'annulation partielle visée en B.9.1 et du maintien des effets visé en B.9.3, le législateur doit, avant la date mentionnée dans le dispositif, inclure dans une disposition législative les données d'identification et les documents d'identification qui peuvent servir à l'application de l'article 127 de la loi du 13 juin 2005.

B.15.3. Ces données personnelles ne sont pas des données relatives au trafic et des données de localisation, mais uniquement les données qui sont habituellement utilisées pour identifier une personne. Il n'est pas possible, à l'aide de ces seules données, de suivre les déplacements, les communications, les activités ou les relations sociales de cette personne, ni d'établir un profil personnel permettant de tirer des conclusions précises sur son orientation sexuelle, ses convictions et son état de santé. En soi, elles ne divulguent donc pas d'informations sensibles sur la vie privée.

Il est exact que ces données d'identification peuvent ensuite être associées à d'autres données et contribuer, de cette manière, à la divulgation de telles informations sensibles sur la vie privée d'une personne. Ces autres données doivent toutefois, dans ce cas, être collectées d'une autre manière et cette collecte doit elle aussi s'effectuer dans le respect de la législation applicable et des droits fondamentaux de l'intéressé.

Par conséquent, il y a lieu d'apprécier la compatibilité de la loi attaquée avec le droit au respect de la vie privée à l'aide des critères mentionnés en B.14.3.

B.16.1. Les conditions matérielles et procédurales de la collecte, du traitement et de la conservation des données d'identification des utilisateurs finaux d'un réseau de communications électroniques sur la base d'une carte de téléphonie mobile prépayée sont réglées dans les articles 126 et 127 de la loi du 13 juin 2005 et dans les arrêtés royaux du 19 septembre 2013 et du 27 novembre 2016.

B.16.2. Comme il est dit en B.2.1 à B.2.7, l'article 127 de la loi du 13 juin 2005 détermine les personnes qui se voient imposer des obligations dans ce cadre, à savoir les opérateurs, les fournisseurs, les canaux de vente de services de communications électroniques, les entreprises qui fournissent un service d'identification et les utilisateurs finaux eux-mêmes. Il désigne également le responsable du traitement des données, à savoir l'opérateur ou le fournisseur. Il définit en outre le principe selon lequel tous les utilisateurs finaux doivent être identifiables, indépendamment du fait qu'ils utilisent une ancienne ou une nouvelle carte de téléphonie mobile prépayée, et dispose que l'identification doit être effectuée sur la base d'un document d'identification comprenant le numéro de registre national.

L'arrêté royal du 27 novembre 2016 oblige les utilisateurs finaux de cartes de téléphonie mobile prépayées à s'identifier auprès de l'opérateur au plus tard lors de l'activation de celles-ci selon l'une des méthodes d'identification valides décrites dans le même arrêté royal et à l'aide d'un des documents d'identification valides mentionnés dans l'arrêté royal. Il a obligé les opérateurs à identifier tous les utilisateurs finaux d'anciennes cartes de téléphonie mobile prépayées avant le 7 juin 2017 et leur interdit d'encore activer de nouvelles cartes prépayées si l'utilisateur final n'a pas encore été identifié. S'ils sont informés par l'utilisateur final de la perte ou du vol de la carte de téléphonie mobile prépayée, ils doivent la rendre immédiatement inutilisable.

En ce qui concerne le traitement des données proprement dit, l'arrêté royal du 27 novembre 2016 dispose que l'opérateur, le fournisseur d'un service d'identification ou le canal de vente de services de communication électroniques lisent électroniquement la carte d'identité électronique belge, en font un scan, une photo ou une copie, en ce compris de la photo se trouvant sur cette carte et du numéro de cette carte. Avant l'activation de la carte de téléphonie mobile prépayée, l'opérateur doit contrôler si la carte d'identité présentée a été volée ou a fait l'objet d'une fraude. Il doit également conserver la méthode d'identification qui a été utilisée pour identifier l'utilisateur final pendant la durée visée à l'article 126 de la loi du 13 juin 2015.

B.16.3. Les parties requérantes ne contestent pas que ces règles sont claires et précises. Elles font seulement valoir que le cadre légal relatif à la conservation des données traitées manque de clarté depuis l'arrêt de la Cour n° 57/2021 du 22 avril 2021, parce que la Cour a annulé dans cet arrêt les règles relatives aux données traitées, aux personnes impliquées dans le traitement, aux conditions et aux finalités du traitement, ainsi que les règles relatives à la Cellule de coordination. De ce fait, il n'existerait plus de conditions matérielles et procédurales réglant le traitement des données ou des documents d'identification conservés.

B.16.4. Comme il est dit en B.8.7.3, l'arrêt n° 57/2021 n'a pas pour effet qu'il n'existe plus de cadre législatif pour la conservation des données d'identification collectées et traitées. L'annulation des articles 2, *b)*, 3 à 11 et 14 de la loi du 29 mai 2016 a seulement pour effet que l'article 126 de la loi du 13 juin 2005 est actuellement applicable, pour ce qui est des données d'identification des utilisateurs de cartes prépayées, dans sa version qui a été modifiée pour la dernière fois par l'article 33 de la loi du 4 février 2010 « relative aux méthodes de recueil des données par les services de renseignement et de sécurité ».

B.16.5. En application de l'article 126 de la loi du 13 juin 2005, l'arrêté royal du 19 septembre 2013 fixe les conditions de conservation des données collectées. Les articles 3 à 6 de cet arrêté déterminent les données qui doivent être conservées et les personnes qui se chargent de la conservation :

« 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. Cet arrêté royal ne fixe toutefois pas de délai de conservation minimal ou maximal des données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005. En effet, ce délai était ancré dans l'article 126, § 3, de la loi du 13 juin 2005, annulé par l'arrêt n° 57/2021, qui disposait :

« Les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication, à l'exclusion des données spécifiquement prévues aux alinéas 2 et 3, sont conservées pendant douze mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

Les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, sont conservées pendant douze mois à partir de la date de la communication.

Les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination, sont conservées pendant douze mois à partir de la date de la communication.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de catégories visées aux alinéas 1 à 3 ainsi que les exigences auxquelles ces données doivent répondre ».

Dans l'attente de l'entrée en vigueur d'une nouvelle version de l'article 126 de la loi du 13 juin 2005, l'utilisateur final d'une carte de téléphonie mobile prépayée n'est toutefois pas soumis à un risque de conservation illimitée de ses données d'identification. En effet, la version actuellement applicable de cette disposition mentionne un délai de conservation maximal de trente-six mois.

Par ailleurs, cet utilisateur final bénéficie de la protection du RGPD, que le responsable du traitement se doit de respecter parallèlement aux dispositions applicables du droit national - et, si nécessaire, en priorité par rapport à celles-ci. En vertu du principe de la limitation de la conservation inscrit dans l'article 5, point *e)*, du RGPD, le responsable du traitement doit conserver les données personnelles « sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Compte tenu de ces dispositions, il peut être admis, dans l'attente de l'entrée en vigueur d'un nouveau cadre législatif en matière de conservation des données, que la législation applicable ne prévoie temporairement pas un délai de conservation spécifique. Dans cette période intermédiaire, il appartient aux juridictions et aux autorités administratives compétentes de garantir, en vertu de ces dispositions, que les données d'identification des utilisateurs finaux de cartes de téléphonie mobile prépayées ne sont pas conservées plus longtemps que ce qui est nécessaire au regard des objectifs poursuivis par l'obligation d'identification attaquée.

B.16.7. Ces objectifs sont énumérés limitativement dans l'article 127, § 1er, de la loi du 13 juin 2005. Il s'agit du bon fonctionnement des services d'urgence, de l'instruction pénale et du fonctionnement des services de renseignement et de sécurité. Ces deuxième et troisième objectifs correspondent aux motifs pour lesquels la Cour de justice autorise la conservation des données d'identification (CJUE, grande chambre, 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, points 152 à 159). Le bon fonctionnement des services d'urgence, quant à lui, est lié aux obligations positives qui incombent aux autorités dans le cadre des droits que les victimes d'infractions et d'accidents puisent dans les articles 2, 3, 5 et 8 de la Convention européenne des droits de l'homme.

B.16.8.1. La législation relative à ces services mentionne en outre de manière limitative les autorités qui ont accès aux données d'identification conservées ainsi que les conditions matérielles et procédurales qu'elles doivent remplir à cette fin.

B.16.8.2. L'accès à ces données dans le cadre d'une information pénale et d'une instruction pénale est réglé par les articles 46*bis*, 88*bis* et 90*ter* à 90*decies* du Code d'instruction criminelle.

L'article 46*bis* du Code d'instruction criminelle dispose :

« § 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients des acteurs visés à l'alinéa 2, premier et deuxième tirets, à :

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, ou bien du moyen de communication électronique utilisé;

2° l'identification des services visés à l'alinéa 2, deuxième tiret, auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration :

- de l'opérateur d'un réseau de communications électroniques, et

- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête.

En cas d'extrême urgence, le procureur du Roi peut ordonner verbalement cette mesure.

La décision est confirmée par écrit dans les plus brefs délais.

Pour des infractions qui ne sont pas de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi ne peut requérir les données visées à l'alinéa 1er que pour une période de six mois préalable à sa décision.

§ 2. Les acteurs visés au § 1er, alinéa 2, 1er et 2e tirets, requis de communiquer les données visées au paragraphe 1er communiquent au procureur du Roi ou à l'officier de police judiciaire les données en temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi, sur proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.

Le Roi fixe, après avis de la Commission de la protection de la vie privée et sur proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications, les conditions techniques d'accès aux données visées au § 1er et disponibles pour le procureur du Roi et le service de police désigné au même paragraphe.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie d'une amende de vingt-six euros à dix mille euros ».

L'article 88*bis* du Code d'instruction criminelle dispose :

« § 1er. S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut faire procéder :

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;

2° à la localisation de l'origine ou de la destination de communications électroniques.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration :

- de l'opérateur d'un réseau de communications électroniques; et

- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

Dans les cas visés à l'alinéa 1er, pour chaque moyen de communication électronique dont les données de trafic sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal.

Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée.

Il précise également la durée durant laquelle la mesure pourra s'appliquer pour le futur, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement et, le cas échéant, la période pour le passé sur laquelle l'ordonnance s'étend conformément au paragraphe 2.

En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90*ter*, §§ 2, 3 et 4. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction.

S'il s'agit toutefois de l'infraction visée à l'article 137, 347*bis*, 434 ou 470 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction ne soit nécessaire.

S'il s'agit de l'infraction visée à l'article 137 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut en outre ordonner la mesure dans les septante-deux heures suivant la découverte de cette infraction, sans qu'une confirmation par le juge d'instruction soit nécessaire.

Toutefois, le procureur du Roi peut ordonner la mesure si le plaignant le sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et § 3*bis* de la loi du 13 juin 2005 relative aux communications électroniques.

En cas d'urgence, la mesure peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue aux alinéas 4 et 5.

§ 2. Pour ce qui concerne l'application de la mesure visée au paragraphe 1er, alinéa 1er, aux données de trafic ou de localisation conservées sur la base de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s'appliquent :

- pour une infraction visée au livre II, titre I*ter*, du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance;

- pour une autre infraction visée à l'article 90*ter*, §§ 2 à 4, qui n'est pas visée au premier tiret ou pour une infraction qui est commise dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal, ou pour une infraction qui est de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde, le juge d'instruction peut dans son ordonnance requérir les données pour une période de neuf mois préalable à l'ordonnance;

- pour les autres infractions, le juge d'instruction ne peut requérir les données que pour une période de six mois préalable à l'ordonnance.

§ 3. La mesure ne peut porter sur les moyens de communication électronique d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une infraction visée au paragraphe 1er ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une infraction visée au paragraphe 1er, utilisent ses moyens de communication électronique.

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas consignés au procès-verbal. Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 4. Les acteurs visés au § 1er, alinéa 2, communiquent les informations demandées en temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées au présent article, concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition, est punie d'une amende de vingt-six euros à dix mille euros ».

L'article 90*ter*, § 1er, du Code d'instruction criminelle dispose :

« Sans préjudice de l'application des articles 39*bis*, 87, 88, 89*bis* et 90, le juge d'instruction peut, dans un but secret, intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre la recherche dans un système informatique ou une partie de celui-ci.

Cette mesure ne peut être ordonnée que dans des cas exceptionnels, lorsque les nécessités de l'instruction l'exigent, s'il existe des indices sérieux que cela concerne une infraction visée au paragraphe 2, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité.

En vue de permettre cette mesure, le juge d'instruction peut également, à l'insu ou sans le consentement de l'occupant, du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment :

- la pénétration dans un domicile, un lieu privé ou un système informatique;

- la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités;

- l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.

La mesure visée au présent paragraphe ne peut être ordonnée que pour rechercher les données qui peuvent servir à la manifestation de la vérité. Elle ne peut être ordonnée qu'à l'égard soit de personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, soit à l'égard des moyens de communication ou systèmes informatiques régulièrement utilisés par un suspect, soit à l'égard des lieux présumés fréquentés par celui-ci. Elle peut également être ordonnée à l'égard de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect ».

B.16.8.3. L'accès à ces données dans le cadre d'une enquête réalisée par les services de renseignement et de sécurité est réglé par l'article 16/2, § 1er, de la loi du 30 novembre 1998, qui dispose :

« Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à :

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé;

2° l'identification des services et des moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

La réquisition est effectuée par écrit par le dirigeant de service ou son délégué. En cas d'urgence, le dirigeant de service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite.

Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis donne au dirigeant de service ou à son délégué les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions.

Le dirigeant de service ou son délégué peut, dans le respect des principes de proportionnalité et de subsidiarité, et moyennant l'enregistrement de la consultation, également obtenir les données visées au moyen d'un accès aux fichiers des clients de l'opérateur ou du fournisseur du service. Le Roi fixe, sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, les conditions techniques auxquelles cet accès est possible ».

B.16.8.4. L'accès à ces données par les services d'urgence est réglé par l'article 107, § 2, de la loi du 13 juin 2005, qui dispose :

« Les opérateurs concernés par un appel d'urgence vers un service d'urgence offrant de l'aide sur place, si nécessaire en se coordonnant entre eux, fournissent aux centrales de gestion de ce service d'urgence, dès que l'appel leur parvient et gratuitement, les données d'identification de l'appelant.

Cette obligation est également d'application lorsque les centrales de gestion des services d'urgence offrant de l'aide sur place sont exploitées par une organisation qui est chargée de cette tâche par les pouvoirs publics.

Les coûts d'investissement et d'exploitation relatifs aux bases de données des données d'identification de l'appelant et aux lignes d'accès utilisées par les services d'urgence pour consulter ces bases de données sont à charge des opérateurs.

Si un opérateur offre ses propres services commerciaux pour la fourniture de données de localisation aux abonnés, alors la précision des données de localisation qui font partie de l'identification de l'appelant lors d'un appel d'urgence et qui doivent être fournies aux services d'urgence offrant de l'aide sur place conformément au présent paragraphe et la vitesse à laquelle elles sont transmises au service d'urgence concerné doivent être au moins égales à la meilleure qualité offerte au niveau commercial par cet opérateur. L'Institut peut définir, en concertation avec les services d'urgence concernés, les critères relatifs à la précision et la fiabilité des données de localisation de l'appelant fournies.

L'identification de l'appelant peut être utilisée par les services d'urgence offrant de l'aide sur place ou par l'organisation qui est chargée de l'exploitation des centrales de gestion des services d'urgence par les pouvoirs publics, à l'aide de mesures administratives et techniques approuvées par le ministre sur l'avis de l'Institut et de la Commission pour la protection de la vie privée, afin de lutter contre les appels malveillants ou l'utilisation abusive des numéros d'urgence. Ces mesures ne peuvent toutefois entraîner une inaccessibilité du numéro d'urgence du service d'urgence en question à partir d'une connexion bien précise pendant une période ininterrompue excédant vingt-quatre heures.

Les centrales de gestion des services d'urgence offrant de l'aide à distance obtiennent gratuitement des opérateurs concernés l'identification de la ligne appelante disponible sur le réseau des opérateurs, afin de pouvoir traiter des appels d'urgence et de lutter contre les appels malveillants, même si l'utilisateur a entrepris des démarches pour empêcher l'envoi de l'identification. Le format d'identification de la ligne appelante fournie doit être conforme aux normes ETSI applicables et est défini par l'Institut en concertation avec les services d'urgence et les opérateurs.

L'identification de la ligne appelante peut être utilisée par les services d'urgence offrant de l'aide à distance, à l'aide de mesures administratives et techniques approuvées par le ministre sur l'avis de l'Institut et de la Commission pour la protection de la vie privée, afin de lutter contre les appels malveillants. Ces mesures ne peuvent toutefois entraîner une inaccessibilité du numéro d'urgence du service d'urgence en question à partir d'une connexion bien précise pendant une période ininterrompue excédant vingt-quatre heures ».

B.16.8.5. Ces dispositions règlent de manière claire et précise les conditions matérielles et procédurales auxquelles ces autorités peuvent avoir accès aux données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005.

Lorsqu'elles accèdent à ces données, ces autorités doivent respecter non seulement les règles mentionnées en B.16.8.2 à B.16.8.4, mais aussi les droits fondamentaux de l'utilisateur final, garantis notamment par le RGPD, par les articles 6 et 8 de la Convention européenne des droits de l'homme et par les articles 7, 8 et 47 de la Charte.

B.16.8.6. À cet égard, les parties requérantes renvoient à l'arrêt de la grande chambre de la Cour de justice du 2 mars 2021 en cause *Prokuratuur* (C-746/18, points 50 à 56), dans lequel la Cour de justice exige, selon elles, qu'une autorité administrative indépendante ou un juge contrôle au préalable chaque demande d'accès au regard des droits fondamentaux et règles nationales applicables et dans lequel elle précise, selon les parties requérantes, que le ministère public, qui dirige la procédure d'enquête et exerce le cas échéant l'action publique, ne dispose pas de l'indépendance requise pour pouvoir effectuer ce contrôle.

Toutefois, cet arrêt portait sur une demande du ministère public d'obtenir un accès à des données relatives au trafic et à des données de localisation. Comme il est dit en B.14.3, la Cour de justice et la Cour européenne des droits de l'homme n'exigent en revanche pas de contrôle judiciaire ou administratif préalable pour une demande d'accès à des données d'identification. En conséquence, le droit au respect de la vie privée ne s'oppose pas à une demande d'accès à de telles données qui émane du ministère public.

B.16.8.7. Cela étant, la demande d'accès aux données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005 doit toujours être motivée *in concreto* par la démonstration du lien entre ces données et les éléments objectifs qui fondent la suspicion concrète initiale à l'égard de l'utilisateur final en question concernant une infraction spécifique. Il faut également motiver le fait que l'on ne demande pas davantage de données que celles qui sont strictement nécessaires dans le cadre de l'enquête en cours. Une telle motivation ne peut pas recourir à des formulations types ou à des formules de style.

B.16.9.1. La loi du 13 juin 2005 et les arrêtés royaux du 19 septembre 2013 et du 26 novembre 2016 contiennent des garanties contre les abus dans le cadre de la collecte, du traitement et de la conservation des données d'identification.

L'article 127, § 1er, de la loi du 13 juin 2005 dispose que le canal de vente de services de communications électroniques transmet les données d'identification et les documents d'identification collectés à l'opérateur, sans conserver lui-même de copies. Si l'introduction directe de ces données dans le système informatique n'est pas possible, le canal de vente peut faire une copie temporaire du document d'identification, qui doit être détruite au plus tard au moment de l'activation de la carte de téléphonie mobile prépayée.

En vertu de l'article 11, § 1er, de l'arrêté royal du 27 novembre 2016, l'entreprise concernée doit systématiquement vérifier si une carte d'identité présentée n'a pas été volée ou n'a pas fait l'objet d'une fraude. En vertu de l'article 12, alinéa 3, du même arrêté royal, l'entreprise concernée ou le fournisseur d'un service d'identification doit détruire la copie de la photo se trouvant sur la carte d'identité électronique au plus tard avant l'activation de la carte de téléphonie mobile prépayée.

En vertu de l'article 8 de l'arrêté royal du 19 septembre 2013, chaque fournisseur doit désigner parmi les membres de la Cellule de Coordination de Justice un préposé à la protection des données à caractère personnel, qui agit dans le cadre de la protection des données à caractère personnel en toute indépendance par rapport à ce fournisseur et qui a accès à toutes les données pertinentes ainsi qu'à tous les locaux pertinents de ce fournisseur. Il doit veiller à ce que tous les traitements poursuivent les objectifs mentionnés à l'article 126 de la loi du 13 juin 2005, que seules les personnes autorisées en vertu de cette disposition et de l'arrêté royal du 19 septembre 2013 aient accès aux données et que toutes les mesures de protection des données décrites à l'article 126 de la loi du 13 juin 2005 soient respectées.

B.16.9.2. En ce qui concerne l'accès aux données conservées, l'article 9 de l'arrêté royal du 19 septembre 2013 dispose que chaque fournisseur communique avant le 1er mars de chaque année à l'Institut belge des services postaux et des télécommunications le nombre de cas dans lesquels des données ont été, au cours de l'année civile écoulée, transmises aux autorités compétentes, le délai écoulé entre le traitement et la demande des données et les cas dans lesquels les demandes de données n'ont pas pu être satisfaites. Cet Institut transmet ces informations annuellement au ministre de la Justice.

En outre, en vertu de l'article 90*decies* du Code d'instruction criminelle, le ministre de la Justice fait rapport annuellement au Parlement sur l'application, notamment, des articles 46*bis*, 88*bis* et 90*ter* à 90*novies* du même Code. Cette communication concerne le nombre d'instructions ayant donné lieu aux mesures visées dans ces articles, la durée de ces mesures, le nombre de personnes concernées et les résultats obtenus.

En vertu de l'article 21 de la loi du 30 novembre 1998, les données à caractère personnel traitées dans le cadre de l'application de cette loi sont conservées par les services de renseignement et de sécurité pour une durée n'excédant pas celle qui est nécessaire aux finalités pour lesquelles elles sont enregistrées.

L'article 126, §§ 4 à 6, de la loi du 13 juin 2005, annulé par l'arrêt de la Cour nº 57/2021, prévoyait encore d'autres garanties contre les abus :

« § 4. Pour la conservation des données visées au paragraphe 3, les fournisseurs et les opérateurs visés au paragraphe 1er, alinéa 1er :

1º garantissent que les données conservées sont de la même qualité et sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau;

2º veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites;

3º garantissent que l'accès aux données conservées pour répondre aux demandes des autorités visées au paragraphe 2 n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 126/1, § 1er;

4º conservent les données sur le territoire de l'Union européenne;

5º mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès;

6º détruisent les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données fixé au paragraphe 3, sans préjudice des articles 122 et 123;

7º assurent une traçabilité de l'exploitation des données conservées pour chaque demande d'obtention de ces données d'une autorité visée au paragraphe 2.

La traçabilité visée à l'alinéa 1er, 7º, s'effectue à l'aide d'un journal. L'Institut et la Commission pour la protection de la vie privée peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal. L'Institut et la Commission pour la protection de la vie privée concluent un protocole de collaboration concernant la prise de connaissance et le contrôle du contenu du journal.

§ 5. Le ministre et le ministre de la Justice font en sorte que des statistiques sur la conservation des données qui sont générées ou traitées dans le cadre de la fourniture de services ou réseaux de communications accessibles au public soient transmises annuellement à la Chambre des représentants.

Ces statistiques comprennent notamment :

1º les cas dans lesquels des données ont été transmises aux autorités compétentes conformément aux dispositions légales applicables;

2º le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission;

3º les cas dans lesquels des demandes de données n'ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel.

Les données qui concernent l'application du paragraphe 2, 1º, sont également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.

Le Roi détermine, sur proposition du ministre de la Justice et du ministre et sur avis de l'Institut, les statistiques que les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au ministre de la Justice.

§ 6. Sans préjudice du rapport visé au paragraphe 5, alinéa 4, le ministre et le ministre de la Justice font un rapport d'évaluation à la Chambre des représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé au paragraphe 3, alinéa 4, sur la mise en œuvre du présent article, afin de vérifier si des dispositions doivent être adaptées, en particulier en ce qui concerne les données à conserver et la durée de la conservation ».

Il appartient au législateur, lorsqu'il créera un nouveau cadre législatif en matière de conservation des données répondant aux critères mentionnés dans l'arrêt nº 57/2021, d'y inclure à nouveau des garanties contre les abus. En attendant qu'il le fasse - et compte tenu des autres garanties contre les abus qui sont mentionnées -, l'absence d'une telle disposition, qui porte uniquement sur l'accès aux données personnelles conservées, ne peut pas conduire à l'annulation de la loi attaquée, qui traite en effet uniquement de la collecte, du traitement et de la conservation initiaux des données d'identification des utilisateurs d'une carte de téléphonie mobile prépayée.

B.16.10. L'article 127 de la loi du 13 juin 2005 ne prévoit pas de contrôle juridictionnel spécifique du traitement des données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005. Toutefois, comme il est dit en B.14.3, les recours de droit commun suffisent en matière de traitement de simples données d'identification et d'accès à celles-ci (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, § 106).

Dans le cadre de la procédure pénale, le prévenu dispose à cet égard du droit d'invoquer devant les juridictions d'instruction ou devant la juridiction de jugement la nullité d'un acte d'instruction qui viole son droit au respect de la vie privée ou son droit à un procès équitable.

Dans le cadre du fonctionnement des services de renseignement et de sécurité, l'intéressé dispose, en vertu de l'article 79 de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », du droit de demander au Comité permanent R de faire rectifier ou supprimer ses données à caractère personnel inexactes et de vérifier le respect des dispositions applicables.

De plus, chaque utilisateur final d'une carte de téléphonie mobile prépayée dont les données d'identification ont été traitées en violation de l'article 127 de la loi du 13 juin 2005 et de l'arrêté royal du 27 novembre 2016 dispose d'une action en responsabilité de droit commun contre la personne qui a enfreint cette disposition législative.

Enfin, l'intéressé peut, en vertu de l'article 58 de la loi du 3 décembre 2017 « portant création de l'Autorité de protection des données », déposer sans frais une plainte auprès de l'Autorité de protection des données en cas de traitement illégitime de ses données à caractère personnel.

B.16.11.1. Les trois objectifs légitimes que le législateur poursuit avec l'article 127 de la loi du 13 juin 2005, à savoir le bon fonctionnement des services d'urgence, la détection, la poursuite et la répression d'infractions et la collecte d'informations par les services de renseignement et de sécurité, sont tous liés aux obligations positives qui incombent aux autorités publiques en matière de droit à la vie, d'interdiction de traitements inhumains et dégradants et de droit à la liberté et à la sécurité de toute la population.

B.16.11.2. Une mesure qui prévoit l'identifiabilité de tous les utilisateurs finaux d'une carte de téléphonie mobile prépayée est pertinente pour atteindre ces objectifs.

La possibilité de céder une carte de téléphonie mobile prépayée et la possibilité qu'elle soit volée ne suffisent pas pour arriver à une autre conclusion. C'est d'ailleurs la raison pour laquelle l'article 127, § 1er, alinéa 3, de la loi du 13 juin 2005 dispose que la personne identifiée est réputée utiliser elle-même le service de communications électroniques. Cette disposition vise à l'inciter à la prudence en ce qui concerne l'utilisation de sa carte de téléphonie mobile prépayée par des tiers. L'article 5 de l'arrêté royal du 27 novembre 2016 limite en outre la possibilité de céder une carte de téléphonie mobile prépayée à des tiers : sauf dans l'hypothèse où la carte de téléphonie mobile est cédée à un proche de la famille (article 5, 1º à 3º), une cession n'est possible que si ce tiers s'identifie au préalable auprès de

l'entreprise concernée (article 5, 4°), si une personne morale qui attribue une carte de téléphonie mobile à une personne physique effectuant des prestations pour elle conserve une liste actualisée des personnes à qui elle a donné une carte (article 5, 5°), ou si la carte de téléphonie mobile est achetée pour le compte des services de renseignement et de sécurité, des services de police ou de certaines autorités désignées par arrêté royal (article 5, 6°). En cas de perte ou de vol de la carte de téléphonie mobile, l'article 6 du même arrêté royal oblige l'utilisateur final à en informer l'entreprise concernée dans les 24 heures.

De même, l'existence d'autres techniques de communication n'empêche pas le législateur de supprimer l'anonymat des cartes de téléphonie mobile prépayées s'il constate notamment que ces cartes de téléphonie mobile sont utilisées dans des milieux terroristes et criminels et que cet anonymat constitue un problème insurmontable pour les autorités judiciaires et pour les services de renseignement et de sécurité. Au demeurant, si la disposition attaquée a pour effet que les organisations terroristes et criminelles passent à des techniques plus avancées, cela démontre plutôt la pertinence de la mesure attaquée. Il appartient alors au législateur de réguler également l'utilisation de ces techniques, en vue de réaliser les mêmes objectifs.

B.16.11.3. Compte tenu des garanties mentionnées en B.16.1 à B.16.9.3, l'identifiabilité de l'utilisateur final d'une carte de téléphonie mobile prépayée, qui doit être considérée comme une mesure présentant une faible incidence sur la vie privée, est également proportionnée au regard de ces objectifs. Le fait que cette mesure porte sur tous les utilisateurs finaux de carte de téléphonie mobile prépayée, même s'ils ne sauraient être suspectés du moindre comportement criminel, n'y change rien, étant donné qu'une mesure d'identifiabilité ne peut fonctionner que pour autant que toute personne puisse être identifiée dès que nécessaire.

B.16.11.4. Enfin, les utilisateurs de cartes de téléphonie mobile prépayées ne pouvaient pas ignorer le fait que l'anonymat de ces cartes de téléphonie mobile serait un jour supprimé. Comme il est dit en B.2.1 à B.2.7, cet anonymat a en effet toujours été conçu comme une exception temporaire à la règle selon laquelle tous les utilisateurs finaux de réseaux de communications électroniques doivent être identifiables.

B.16.12. Sous réserve des interprétations mentionnées en B.8.7.3, B.16.6, B.16.8.5 et B.16.8.7, le deuxième moyen, en sa première branche, n'est pas fondé.

En ce qui concerne la deuxième branche du deuxième moyen

B.17. Dans la deuxième branche du deuxième moyen, les parties requérantes font valoir que la loi attaquée viole la liberté d'établissement et la libre prestation des services.

B.18. Toute mesure nationale qui peut avoir pour effet de gêner ou de rendre moins attrayante la libre prestation des services par des entreprises d'un autre État membre de l'Union européenne constitue une restriction de la libre prestation de services. Par ailleurs, l'article 56 du Traité sur le fonctionnement de l'Union européenne accorde des droits non seulement au prestataire des services, mais aussi au destinataire de ceux-ci.

Une telle restriction peut toutefois être justifiée par des « raisons impérieuses d'intérêt général, à condition qu'elles soient propres à garantir la réalisation de l'objectif poursuivi et qu'elles n'aillent pas au-delà de ce qui est nécessaire pour atteindre cet objectif, à savoir s'il n'existe pas des mesures moins restrictives qui permettraient de l'atteindre de manière aussi efficace » (CJUE, 11 février 2021, C-407/19 et C-471/19, *Katoen Natie Bulk Terminals NV e.a.*, points 59 à 61).

B.19.1. Sans qu'il soit nécessaire d'examiner si la loi attaquée restreint la liberté d'établissement ou la libre prestation de services, il suffit de constater qu'elle est justifiée par des raisons impérieuses d'intérêt général, à savoir le bon fonctionnement des services d'urgence, la détection, la poursuite et la répression efficaces d'infractions pénales et la prévention d'activités terroristes, en assurant que les services de renseignement et de sécurité puissent associer des menaces éventuelles à l'identité de personnes dont des communications ont été interceptées.

B.19.2. Comme il est dit en B.16.11.2, la loi attaquée est pertinente eu égard à ces objectifs. De plus, elle ne va pas au-delà de ce qui est nécessaire pour les atteindre. Une mesure qui vise à assurer que les utilisateurs finaux d'un réseau de communications électroniques belge soient identifiables ne peut en effet être utile que si elle est applicable sans exception à tous les utilisateurs finaux de ce réseau, indépendamment du fait qu'ils téléphonent au moyen d'un abonnement ou d'une carte de téléphonie mobile prépayée, que cette carte ait déjà été achetée avant l'entrée en vigueur de la loi attaquée ou non et qu'il s'agisse d'une carte de téléphonie fournie par une entreprise établie en Belgique ou dans un autre État membre de l'Union européenne.

L'exclusion des cartes de téléphonie mobile prépayées fournies par des entreprises établies dans un autre État membre du champ d'application de l'article 127 de la loi du 13 juin 2005 rendrait l'identifiabilité impossible dans la pratique, étant donné, notamment, que des personnes mal intentionnées pourraient aisément s'y soustraire en achetant une carte de téléphonie mobile prépayée d'une entreprise établie dans un autre État membre.

B.19.3. Le deuxième moyen, en sa deuxième branche, n'est pas fondé.

En ce qui concerne la troisième branche du deuxième moyen

B.20. Dans la troisième branche du deuxième moyen, les parties requérantes font valoir que la loi attaquée viole la liberté d'expression, étant donné que l'identifiabilité des utilisateurs finaux d'une carte de téléphonie mobile prépayée les dissuaderait d'informer des personnalités politiques et des journalistes et limiterait ainsi de manière disproportionnée la liberté de recevoir des informations et des idées ainsi que le secret des sources des journalistes.

B.21.1. La liberté d'expression constitue l'un des fondements essentiels d'une société démocratique. Elle vaut non seulement pour les « informations » ou « idées » accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui « choquent, inquiètent ou heurtent » l'État ou une fraction de la population. Ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans lesquels il n'est pas de société démocratique (CEDH, 7 décembre 1976, *Handyside c. Royaume-Uni*, § 49; 23 septembre 1998, *Lehideux et Isorni c. France*, § 55; 28 septembre 1999, *Öztürk c. Turquie*, § 64; grande chambre, 13 juillet 2012, *Mouvement Raëlien suisse c. Suisse*, § 48).

Ainsi qu'il ressort des termes de l'article 10, paragraphe 2, de la Convention européenne des droits de l'homme, l'exercice de la liberté d'expression implique néanmoins certaines obligations et responsabilités (CEDH, 4 décembre 2003, *Gündüz c. Turquie*, § 37), notamment le devoir de principe de ne pas franchir certaines limites « tenant notamment à la protection de la réputation et aux droits d'autrui » (CEDH, 24 février 1997, *De Haes et Gijsels c. Belgique*, § 37; 21 janvier 1999, *Fressoz et Roire c. France*, § 45; 15 juillet 2003, *Ernst e.a. c. Belgique*, § 92). La liberté d'expression peut, en vertu de l'article 10, paragraphe 2, de la Convention européenne des droits de l'homme, être soumise, sous certaines conditions, à certaines formalités, conditions, restrictions ou sanctions, en vue, notamment, de la protection de la réputation ou des droits d'autrui. Les exceptions dont il est assorti appellent toutefois « une interprétation étroite, et le besoin de la restreindre doit se trouver établi de manière convaincante » (CEDH, grande chambre, 20 octobre 2015, *Pentikäinen c. Finlande*, § 87).

L'article 19 de la Constitution interdit que la liberté d'expression soit soumise à des restrictions préventives, mais non que les infractions qui sont commises à l'occasion de la mise en œuvre de cette liberté soient sanctionnées.

B.21.2. Le droit au secret des sources journalistiques doit être garanti, non pas pour protéger les intérêts des journalistes en tant que groupe professionnel, mais bien pour permettre à la presse de jouer son rôle de « chien de garde » et d'informer le public sur des questions d'intérêt général. Pour ces motifs, ce droit fait partie de la liberté d'expression et de la liberté de la presse.

B.21.3. Selon la Cour de justice, « une transmission des données relatives au trafic et des données de localisation à des autorités publiques à des fins sécuritaires est susceptible [...] d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs [...] de leur liberté d'expression, garantie à l'article 11 de la Charte. De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alertes dont les activités sont protégées par la directive (UE) 2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (*JO*, 2019, L-305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés » (CJUE, grande chambre, 6 octobre 2020, C-623/17, *Privacy international*, point 72; voir dans le même sens CJUE, grande chambre, 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland e.a.*, point 28; 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige e.a.*, point 101; 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 118).

B.22. L'article 127 de la loi du 13 juin 2005 porte uniquement sur la conservation et le traitement des données d'identification visées à l'article 12 de l'arrêté royal du 27 novembre 2016. À elles seules, ces données ne donnent pas d'information sur les opinions personnelles de la personne identifiée. De même, les données relatives au trafic et les données de localisation auxquelles elles pourraient être associées ne constituent pas en soi l'expression d'une opinion.

Ce n'est que si ces données étaient également liées au contenu d'une communication effectuée et que l'analyse de celles-ci entraînait d'autres mesures, telles qu'une enquête par les services de renseignement et de sécurité ou une instruction pénale, qu'il pourrait en résulter une limitation de la liberté d'expression, de la liberté d'obtenir des informations, de la liberté de presse ou du secret des sources.

Comme il est dit en B.15.3, une association des données d'identification à d'autres métadonnées ou au contenu d'une communication doit toutefois être fondée sur une disposition législative claire et sans équivoque, respecter les conditions matérielles et procédurales de cette disposition et être compatible avec les droits fondamentaux de l'intéressé.

Un tel lien indirect entre la suppression, attaquée, de l'anonymat des cartes de téléphonie mobile prépayées et le contenu des communications effectuées ne suffit pas pour considérer que la loi attaquée limite la liberté d'expression. La simple collecte de données d'identification de tous les utilisateurs finaux d'un réseau de communications électroniques ne saurait justifier la crainte, dans un État de droit démocratique, que toutes les communications menées sur ce réseau seront supervisées par les pouvoirs publics. La loi attaquée ne saurait dès lors avoir pour effet, par elle-même, de dissuader des personnes d'exprimer leur opinion ou de partager des informations avec des journalistes ou avec des personnalités politiques.

Le deuxième moyen, en sa troisième branche, n'est pas fondé.

Quant au troisième moyen

B.23. Les parties requérantes prennent un troisième moyen de la violation, par l'article 2, 1°, *c)*, de la loi attaquée, des articles 10, 11, 12 et 14 de la Constitution, lus en combinaison avec les articles 6 et 7 de la Convention européenne des droits de l'homme, avec les articles 48, 49 et 52 de la Charte, avec le droit à un procès équitable, avec la présomption d'innocence et avec le principe de légalité en matière pénale, en ce que la présomption, contenue dans cette disposition, d'imputabilité de la communication à l'utilisateur final de la carte de téléphonie mobile prépayée qui a été identifié peut avoir pour effet de rendre cette personne responsable de faits qu'elle n'a pas commis.

B.24.1. L'article 12 de la Constitution dispose :

« La liberté individuelle est garantie.

Nul ne peut être poursuivi que dans les cas prévus par la loi, et dans la forme qu'elle prescrit.

Hors le cas de flagrant délit, nul ne peut être arrêté qu'en vertu d'une ordonnance motivée du juge qui doit être signifiée au plus tard dans les quarante-huit heures de la privation de liberté et ne peut emporter qu'une mise en détention préventive ».

L'article 14 de la Constitution dispose :

« Nulle peine ne peut être établie ni appliquée qu'en vertu de la loi ».

L'article 7 de la Convention européenne des droits de l'homme dispose :

« 1. Nul ne peut être condamné pour une action ou une omission qui, au moment où elle a été commise, ne constituait pas une infraction d'après le droit national ou international. De même il n'est infligé aucune peine plus forte que celle qui était applicable au moment où l'infraction a été commise.

2. Le présent article ne portera pas atteinte au jugement et à la punition d'une personne coupable d'une action ou d'une omission qui, au moment où elle a été commise, était criminelle d'après les principes généraux de droit reconnus par les nations civilisées ».

L'article 49 de la Charte dispose :

« 1. Nul ne peut être condamné pour une action ou une omission qui, au moment où elle a été commise, ne constituait pas une infraction d'après le droit national ou le droit international. De même, il n'est infligé aucune peine plus forte que celle qui était applicable au moment où l'infraction a été commise. Si, postérieurement à cette infraction, la loi prévoit une peine plus légère, celle-ci doit être appliquée.

2. Le présent article ne porte pas atteinte au jugement et à la punition d'une personne coupable d'une action ou d'une omission qui, au moment où elle a été commise, était criminelle d'après les principes généraux reconnus par l'ensemble des nations.

3. L'intensité des peines ne doit pas être disproportionnée par rapport à l'infraction ».

B.24.2. En attribuant au pouvoir législatif la compétence pour déterminer dans quels cas des poursuites pénales sont possibles, l'article 12, alinéa 2, de la Constitution garantit à tout justiciable qu'aucun comportement ne sera punissable qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

En outre, le principe de légalité en matière pénale qui découle de la disposition constitutionnelle précitée procède de l'idée que la loi pénale doit être formulée en des termes qui permettent à chacun de savoir, au moment où il adopte un comportement, si celui-ci est ou non punissable. Il exige que le législateur indique, en des termes suffisamment précis, clairs et offrant la sécurité juridique, quels faits sont sanctionnés, afin, d'une part, que celui qui adopte un comportement puisse évaluer préalablement, de manière satisfaisante, quelle sera la conséquence pénale de ce comportement et afin, d'autre part, que ne soit pas laissé au juge un trop grand pouvoir d'appréciation.

Toutefois, le principe de légalité en matière pénale n'empêche pas que la loi attribue un pouvoir d'appréciation au juge. Il faut en effet tenir compte du caractère de généralité des lois, de la diversité des situations auxquelles elles s'appliquent et de l'évolution des comportements qu'elles répriment.

La condition qu'une infraction doit être clairement définie par la loi se trouve remplie lorsque le justiciable peut savoir, à partir du libellé de la disposition pertinente et, au besoin, à l'aide de son interprétation par les juridictions, quels actes et omissions engagent sa responsabilité pénale.

Ce n'est qu'en examinant une disposition pénale spécifique qu'il est possible de déterminer, en tenant compte des éléments propres aux infractions qu'elle entend réprimer, si les termes généraux utilisés par le législateur sont à ce point vagues qu'ils méconnaîtraient le principe de légalité en matière pénale.

B.24.3. La disposition attaquée n'incrimine aucun comportement et ne définit pas de peines pour des infractions spécifiques. Contrairement à ce que les parties requérantes font valoir, elle n'impute pas non plus automatiquement à l'utilisateur final d'une carte de téléphonie mobile prépayée qui a été identifié les infractions qui sont découvertes ou prouvées à la suite de l'analyse de l'utilisation de cette carte de téléphonie mobile.

L'article 127, § 1er, alinéa 3, de la loi du 13 juin 2005 contient seulement la présomption réfragable selon laquelle cet utilisateur final est également celui qui utilise cette carte de téléphonie mobile. Le principe de légalité en matière pénale n'est pas applicable à une telle disposition.

B.25. L'article 6, paragraphe 2, de la Convention européenne des droits de l'homme dispose :

« Toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie ».

L'article 48, paragraphe 1, de la Charte dispose :

« Tout accusé est présumé innocent jusqu'à ce que sa culpabilité ait été légalement établie ».

Conformément à ces dispositions, toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie.

Les présomptions légales ne sont en principe pas contraires à la présomption d'innocence (voir en ce sens : CEDH, 7 octobre 1988, *Salabiaku c. France*, § 28; 20 mars 2001, *Telfner c. Autriche*, § 16). Elles doivent toutefois être raisonnablement proportionnées au but légitime poursuivi (CEDH, 23 juillet 2002, *Janosevic c. Suède*, § 101; 23 juillet 2002, *Västberga Taxi Aktiebolag et Vulic c. Suède*, § 113), en prenant en compte la gravité de l'enjeu et en préservant les droits de la défense (CEDH, 4 octobre 2007, *Anghel c. Roumanie*, § 60).

B.26.1. À l'origine, l'avant-projet qui a donné lieu à la loi attaquée disposait que la personne identifiée était « responsable » de l'utilisation du service de communications électroniques qui lui était fourni. Dans l'avis nº 59.423/4 du 15 juin 2016, la section de législation du Conseil d'État a formulé l'observation suivante à ce sujet :

« 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 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 46-47).

Compte tenu de cet avis, le législateur a supprimé du projet toute référence à la « responsabilité » de l'utilisateur final. Lors des travaux préparatoires, la version finale de la disposition attaquée a été commentée comme suit :

« 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 » (*ibid.*, p. 9).

B.26.2. La disposition attaquée n'établit dès lors pas de responsabilité pénale automatique ou de responsabilité objective de l'utilisateur final d'une carte de téléphonie mobile prépayée qui a été identifié en ce qui concerne l'utilisation qu'en fait un tiers. Elle remplit principalement une fonction d'avertissement, étant donné qu'elle rappelle la présomption de départ de toute enquête pénale et de toute enquête par les services de renseignement et de sécurité, à savoir la présomption selon laquelle c'est le propriétaire ou l'utilisateur habituel d'un objet qui l'a utilisé pour commettre l'infraction ou pour menacer la sécurité nationale. Les enquêteurs écartent cette présomption dès qu'elle est infirmée par les éléments de preuve recueillis.

Par ailleurs, il convient de lire la disposition attaquée, comme il est dit en B.16.11.2, en combinaison avec les articles 5 et 6 de l'arrêté royal du 27 novembre 2016, qui limitent la possibilité de céder la carte de téléphonie mobile prépayée et qui obligent l'utilisateur final à signaler à l'opérateur la perte ou le vol de cette carte dans les 24 heures. L'ensemble de ces dispositions contribue à la pertinence de l'article 127 de la loi du 13 juin 2005, puisque le but est de faciliter l'identifiabilité du véritable utilisateur d'une carte de téléphonie mobile prépayée.

B.26.3. La disposition attaquée est donc en rapport avec les objectifs que poursuit le législateur par l'article 127 de la loi du 13 juin 2005, à savoir ceux qui portent sur des situations et des enquêtes urgentes.

B.26.4. En outre, la disposition attaquée est souvent appliquée dans le cadre d'infractions ou de menaces pour la sécurité nationale susceptibles d'avoir des conséquences graves sur l'intégrité physique de personnes ou de causer des troubles sociétaux considérables.

B.26.5. L'utilisateur final identifié dispose de plusieurs possibilités pour se défendre dans le cadre des poursuites pénales qui pourraient découler de l'utilisation de sa carte de téléphonie mobile prépayée faite par un tiers. S'il informe les enquêteurs de la personne qui a utilisé sa carte de téléphonie mobile prépayée, ceux-ci doivent examiner l'implication de cette personne.

Du reste, la disposition attaquée se contente d'instaurer une présomption réfragable, que le prévenu peut contester par toutes voies de droit. Elle ne lui interdit pas de présenter tous les éléments de fait qui infirment son implication dans les infractions commises ou dans les menaces pour la sécurité nationale qui font l'objet d'une enquête.

Par ailleurs, la disposition attaquée n'enlève rien au principe selon lequel il revient au ministère public, dans un procès pénal, de prouver la culpabilité du prévenu. Il appartient au juge répressif d'apprécier la valeur probante de tous les éléments de preuve, en ce compris les explications du prévenu, en respectant son droit à un procès équitable.

La disposition attaquée ne portant donc pas atteinte aux droits de défense du prévenu, elle ne compromet pas non plus la présomption d'innocence.

B.26.6. Contrairement à ce que les parties requérantes font valoir, ce qui précède vaut tout autant pour l'implication de l'utilisateur final identifié dans les infractions terroristes mentionnées aux articles 137 à 141*ter* du Code pénal. Il ne peut être condamné en tant que coauteur ou complice de telles infractions que si le ministère public démontre à son encontre que tous les éléments constitutifs de ces infractions, y compris l'élément intentionnel, sont réunis en ce qui le concerne.

La mise à disposition de bonne foi d'une carte de téléphonie mobile prépayée par un utilisateur final qui ne pouvait pas présumer qu'elle serait utilisée pour commettre ou pour préparer une telle infraction ne saurait justifier en soi une condamnation pénale.

B.26.7. Sous réserve des interprétations mentionnées en B.26.2 et B.26.6, le troisième moyen n'est pas fondé.

Quant au quatrième moyen

B.27.1. Les parties requérantes prennent un quatrième moyen de la violation, par l'article 3 de la loi attaquée, des articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte, avec les articles 2, point *a)*, 6, 13 et 22 de la directive 95/46/CE et avec les articles 1er, 2, 3, 5, 6, 9 et 15 de la directive 2002/58/CE. Ce moyen est subdivisé en cinq branches.

B.27.2. Dans la première branche, les parties requérantes font valoir que la disposition attaquée donne aux services de renseignement et de sécurité un accès aux données d'identification collectées sur la base de l'article 127 de la loi du 13 juin 2005, sans limiter cet accès aux infractions graves.

Dans la deuxième branche, elles soutiennent que cet accès des services de renseignement et de sécurité n'est pas soumis à un contrôle préalable effectué par une juridiction ou par une autorité administrative indépendante.

Dans la troisième branche, elles reprochent à la disposition attaquée de ne pas préciser suffisamment les conditions matérielles et procédurales de cet accès.

Dans la quatrième branche, elles déplorent le fait que la disposition attaquée n'oblige pas les services de renseignement et de sécurité qui ont accès aux données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005 à en informer l'intéressé, de sorte qu'il puisse exercer son droit à un contrôle juridictionnel effectif.

Dans la cinquième branche, les parties requérantes font valoir que la disposition attaquée n'exclut pas que des services de renseignement et de sécurité étrangers aient accès à ces données.

Eu égard à leur connexité, ces branches doivent être traitées conjointement.

B.28.1. En vertu de l'article 1er, paragraphe 3, de la directive 2002/58/CE, cette dernière « ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal ».

En vertu de l'article 2, paragraphe 2, point *a)*, du RGPD, ce règlement « ne s'applique pas au traitement de données à caractère personnel effectué dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ». En vertu de l'article 2, paragraphe 2, point *d)*, du RGPD, il ne s'applique pas non plus au traitement des données à caractère personnel effectué par les autorités compétentes à des fins de protection et de prévention des menaces pour la sécurité publique.

Par son arrêt du 6 octobre 2020 en cause *La Quadrature du Net e.a.* (C-511/18, C-512/18 et C-520/18), la grande chambre de la Cour de justice a jugé :

« 135. À cet égard, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme ».

B.28.2. La disposition attaquée insère dans la loi du 30 novembre 1998 un nouvel article 16/2, § 2. En vertu de cette disposition, les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte de téléphonie mobile prépayée sur la base de la référence d'une transaction bancaire électronique qui est liée à cette carte de téléphonie mobile et qui a préalablement été communiquée par l'entreprise concernée.

B.28.3. Étant donné que la disposition attaquée n'est applicable que dans le cadre des missions des services de renseignement et de sécurité, elle ne relève pas du champ d'application du droit de l'Union européenne. Le moyen est dès lors irrecevable en ce qu'il est pris de la violation des dispositions invoquées de la Charte, du RGPD ou de la directive 2002/58/CE.

B.29.1. L'accès d'une autorité aux données bancaires relève du champ d'application du droit au respect de la vie privée, indépendamment du fait que ces données soient sensibles ou non ou qu'elles aient un rapport ou non avec l'exercice de la profession (CEDH, 7 juillet 2005, *M.N. e.a. c. Saint-Marin*, §§ 51-55; 1er décembre 2015, *Brito Ferrinho Bexiga Villa-Nova c. Portugal*, § 44; 27 avril 2017, *Sommer c. Allemagne*, § 48).

B.29.2. L'accès de l'autorité publique aux données bancaires doit être basé sur une habilitation légale spécifique qui en délimite clairement et sans équivoque l'objet ainsi que le seuil pour y accéder. Cet objet doit être limité à ce qui est nécessaire au regard de l'objectif légitime poursuivi, étant donné qu'un accès trop large aux données bancaires permettrait à l'autorité publique de se faire une idée détaillée de la vie privée de l'intéressé. L'autorité publique ne peut avoir accès à de telles données que si elle dispose d'indices concrets que le titulaire du compte bancaire est impliqué dans une infraction. La loi doit également prévoir des mesures contre les abus, parmi lesquelles la garantie que les données ne seront pas conservées plus longtemps que ce qui est nécessaire aux fins de l'investigation menée. Enfin, il doit exister un contrôle juridictionnel effectif du respect de ces garanties matérielles et procédurales (CEDH, 27 avril 2017, *Sommer c. Allemagne*, §§ 57-63).

B.30.1. La disposition attaquée précise les services qui disposent de l'habilitation visée en B.28.2 et les institutions qui sont tenues d'apporter leur concours.

Elle délimite également de deux manières l'objectif de la mesure attaquée. Premièrement, elle vise à identifier soit l'utilisateur final d'une carte de téléphonie mobile prépayée visé à l'article 127 de la loi du 13 juin 2005, soit la carte de téléphonie mobile prépayée qui est utilisée par une certaine personne. Deuxièmement, cette identification doit s'inscrire dans le cadre des missions des services de renseignement et de sécurité.

B.30.2. L'objet de l'acte d'investigation est limité à une transaction bancaire spécifique, à savoir celle qui a permis d'acheter une carte de téléphonie mobile prépayée. Un tel acte d'investigation ne permet aux services de renseignement et de sécurité que de recueillir des données d'identification, mais ne leur fournit pas à lui seul des données relatives au trafic ou des données de localisation, ni un accès aux communications effectuées.

La disposition attaquée ne leur permet pas non plus d'obtenir, par ce seul acte d'investigation, d'autres informations financières relatives au titulaire du compte bancaire. Elle ne leur permet donc pas, à l'aide des seules données d'identification obtenues, de se faire une idée de ses habitudes de dépenses faites par le titulaire du compte bancaire ou de toute autre information personnelle sensible le concernant.

Comme il est dit en B.15.3, s'il est vrai que ces données d'identification peuvent ensuite être associées à d'autres données et que la disposition attaquée peut ainsi contribuer à la divulgation de telles informations sensibles, ces informations doivent alors être recueillies à l'aide d'autres actes d'investigation, qui doivent à leur tour respecter la législation applicable et les droits fondamentaux de l'intéressé.

B.30.3. Comme il est dit en B.3.3, l'identification sur la base de la disposition attaquée peut s'avérer nécessaire en fonction de la méthode d'identification que l'utilisateur final a choisie lors de l'achat de la carte de téléphonie mobile prépayée.

Si, lors de l'achat de la carte de téléphonie mobile prépayée, il opte pour l'identification sur la base de l'opération de paiement en ligne, les services de renseignement et de sécurité ne peuvent l'identifier que s'ils disposent de la référence de la transaction bancaire électronique et qu'ils peuvent l'associer tant à la carte de téléphonie mobile qu'à l'identité de l'utilisateur final (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 14-16). Cette méthode d'identification est réglée à l'article 17 de l'arrêté royal du 27 novembre 2016, qui dispose :

« § 1er. L'entreprise concernée peut identifier l'utilisateur final sur la base d'une opération de paiement électronique en ligne spécifique à l'achat ou la recharge de la carte prépayée.

Cette méthode est soumise aux conditions suivantes :

1° l'opération de paiement doit être traitée par un prestataire de services de paiement tel que visé à l'art. I.9. 2°, *a), b), c),* et *d)* du Code de droit économique;

2° Le prestataire de services de paiement est soumis à la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme;

3° une nouvelle identification doit être effectuée dans les 18 mois qui suivent l'opération de paiement liée à la carte prépayée;

4° l'utilisateur final introduit sur un formulaire en ligne de l'entreprise concernée au minimum son nom, son prénom et le lieu et la date de sa naissance.

§ 2. L'entreprise concernée conserve la référence de l'opération de paiement et les données du formulaire en ligne ».

B.30.4. Étant donné que la disposition attaquée n'habilite les services de renseignement et de sécurité qu'à effectuer l'acte d'investigation attaqué « dans l'intérêt de l'exercice de leurs missions », ceux-ci doivent toujours disposer, à cet effet, d'indices concrets que l'identification de l'utilisateur final d'une carte de téléphonie mobile prépayée est nécessaire dans le cadre des missions énumérées limitativement à l'article 7 (Sûreté de l'État) et à l'article 11 (Service général du renseignement et de la sécurité) de la loi du 30 novembre 1998. Ces missions portant toutes sur des intérêts vitaux de la Nation, le fait de prendre une telle mesure suppose toujours au moins un risque que se produise un événement qui aurait des conséquences sociétales très graves.

B.30.5. La disposition attaquée garantit que la réquisition émane du dirigeant de service ou de son délégué et qu'elle est effectuée par écrit ou confirmée par écrit dans les 24 heures. Par ailleurs, l'article 16/2, § 4, de la loi du 30 novembre 1998 exige que les services de renseignement et de sécurité tiennent un registre de toutes les identifications requises. Ils doivent transmettre cette liste tous les mois au Comité permanent R.

À cet égard, les parties requérantes font valoir que la disposition attaquée n'exige pas que la réquisition du dirigeant de service ou de son délégué soit motivée. Cependant, une telle obligation compromettrait le secret et l'efficacité des enquêtes menées par les services de renseignement et de sécurité.

B.30.6. La disposition attaquée ne garantit pas de contrôle judiciaire spécifique de la mesure d'enquête attaquée. Toutefois, comme il est dit en B.14.3, en matière de traitement et d'accès à de simples données d'identification, les voies de recours de droit commun suffisent (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, § 106). À cet égard, l'intéressé dispose des voies de recours mentionnées en B.16.10.

B.30.7. Étant donné que l'acte d'investigation attaqué constitue une méthode ordinaire de collecte de données, la surveillance par la commission administrative visée à l'article 43/1 de la loi du 30 novembre 1998 et le contrôle *a posteriori* par le Comité permanent R visé aux articles 43/2 à 43/8 de la loi du 30 novembre 1998 n'y sont pas applicables.

Compte tenu de la portée limitée de la disposition attaquée, de l'intérêt fondamental de la sécurité nationale, du fait que la mesure attaquée ne permet aux services de renseignement et de sécurité que d'obtenir des données d'identification, et des garanties mentionnées en B.30.5, cette absence de surveillance ne suffit pas pour conclure que la disposition attaquée violerait le droit au respect de la vie privée.

B.30.8. Les parties requérantes font valoir en outre que, par les arrêts nos 145/2011 du 22 septembre 2011 et 41/2019 du 14 mars 2019, la Cour a obligé le législateur à prévoir une obligation active de notification de la part des services de renseignement et de sécurité à quiconque a fait l'objet d'une enquête effectuée par ces services dès que le secret de l'enquête est levé.

Cependant, la Cour n'a imposé cette obligation qu'en ce qui concerne les méthodes exceptionnelles de collecte de données visées aux articles 18/12, 18/14 et 18/17 de la loi du 30 novembre 1998, qui permettent aux services de renseignement et de sécurité de prendre connaissance du contenu de communications. À cet égard, elle a considéré que ces méthodes étaient les plus intrusives dans la vie privée de l'intéressé. En revanche, elle n'a pas formulé cette exigence pour ce qui est des méthodes ordinaires de collecte de données ni des actes d'investigation qui portent seulement sur la collecte de données d'identification.

B.30.9. En ce que les parties requérantes font valoir enfin que la disposition attaquée permet aux services de renseignement et de sécurité de partager avec des services de renseignement et de sécurité étrangers les données d'identification recueillies, il suffit de constater qu'une telle collaboration ne fait pas l'objet de la disposition attaquée, mais de l'article 20 de la loi du 30 novembre 1998, qui n'est pas attaqué par les parties requérantes.

B.30.10. Sous réserve de l'interprétation mentionnée en B.30.4, le quatrième moyen n'est pas fondé.

Par ces motifs,

la Cour,

- annule l'article 2 de la loi du 1er septembre 2016 « portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité », uniquement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération;

- maintient les effets de la disposition annulée jusqu'à l'entrée en vigueur d'une norme législative qui énumère ces données d'identification et ces documents d'identification et au plus tard jusqu'au 31 décembre 2022 inclus;

- rejette le recours pour le surplus, sous réserve des interprétations mentionnées en B.8.7.3, B.16.6, B.16.8.5, B.16.8.7, B.26.2, B.26.6 et B.30.4.

Ainsi rendu en langue néerlandaise, en langue française et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 18 novembre 2021.

Le greffier, Le président,

P.-Y. Dutilleux L. Lavrysen

VERFASSUNGSGERICHTSHOF

[2021/205605]

Auszug aus dem Entscheid Nr. 158/2021 vom 18. November 2021

Geschäftsverzeichnisnummer 6672

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.

(...)

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 nº 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;

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

6º 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

FEDERAAL AGENTSCHAP VOOR GENEESMIDDELEN EN GEZONDHEIDSPRODUCTEN

[C − 2022/30813]

8 FEBRUARI 2022. — Wet houdende wijziging van de wet van 20 juli 2006 betreffende de oprichting en de werking van het federaal agentschap voor geneesmiddelen en gezondheidsproducten (1)

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen hetgeen volgt :

TITEL I. — ***Inleidende bepaling***

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

TITEL II. — ***Wijzigingen aan de wet van 20 juli 2006 betreffende de oprichting en de werking van het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten***

Art. 2. In artikel 2, § 1, van de wet van 20 juli 2006 betreffende de oprichting en de werking van het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten, laatstelijk gewijzigd bij de wet van 9 mei 2021, worden de volgende wijzigingen aangebracht:

1° de bepalingen onder 2°/1, 2°/2, 2°/3, 2°/4 en 2°/5 worden ingevoegd, luidende:

"2°/1 "geneesmiddel": een geneesmiddel voor menselijk gebruik of een diergeneesmiddel, inclusief homeopathische geneesmiddelen en kruidengeneesmiddelen;"

"2°/2 "geneesmiddel voor menselijk gebruik": een geneesmiddel, zoals bedoeld in artikel 1, § 1, van de wet van 25 maart 1964 op de geneesmiddelen voor menselijk gebruik;

2°/3 "diergeneesmiddel": een geneesmiddel, zoals bedoeld in artikel 4, 1), van Verordening (EU) 2019/6 van het Europees Parlement en de Raad van 11 december 2018 betreffende diergeneesmiddelen en tot intrekking van richtlijn 2001/82/EG;

2°/4 "homeopathisch geneesmiddel":

— een homeopathisch geneesmiddel voor menselijk gebruik, zoals bedoeld in artikel 1, § 1, 5), van de wet van 25 maart 1964 op de geneesmiddelen voor menselijk gebruik; of

— een homeopathisch diergeneesmiddel, zoals bedoeld in artikel 4, punt 10), van vermelde Verordening 2019/6;

2°/5 "een kruidengeneesmiddel": een geneesmiddel voor menselijk gebruik, zoals bedoeld in artikel 1, § 1, 6), van de wet van 25 maart 1964 op de geneesmiddelen voor menselijk gebruik;";

2° de bepaling onder 3° wordt vervangen als volgt:

"3° "magistrale bereiding":

— een geneesmiddel voor menselijk gebruik, bereid in een apotheek overeenkomstig een medisch voorschrift en bestemd voor een welbepaalde patiënt, of

— een diergeneesmiddel, bereid in een apotheek overeenkomstig een diergeneeskundig voorschrift voor een welbepaald dier of kleine groep van dieren;"

AGENCE FEDERALE DES MEDICAMENTS ET DES PRODUITS DE SANTE

[C − 2022/30813]

8 FEVRIER 2022. — Loi modifiant la loi du 20 juillet 2006 relative à la création et au fonctionnement de l'agence fédérale des médicaments et des produits de santé (1)

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

La Chambre des représentants a adopté et Nous sanctionnons ce qui suit :

TITRE Ier. — ***Disposition introductive***

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

TITRE II. — ***Modifications à la loi du 20 juillet 2006 relative à la création et au fonctionnement de l'Agence fédérale des médicaments et des produits de santé***

Art. 2. À l'article 2, § 1er, de la loi du 20 juillet 2006 relative à la création et au fonctionnement de l'Agence fédérale des médicaments et des produits de santé, modifié en dernier lieu par la loi du 9 mai 2021, les modifications suivantes sont apportées:

1° les 2°/1, 2°/2, 2°/3, 2°/4 et 2°/5 sont insérés, rédigés comme suit:

"2°/1 "médicament": un médicament à usage humain ou un médicament vétérinaire, en ce compris les médicaments homéopathiques et les médicaments à base de plantes;"

"2°/2 "médicament à usage humain": un médicament tel que visé à l'article 1er, § 1er de la loi du 25 mars 1964 sur les médicaments à usage humain;

2°/3 "médicament vétérinaire": un médicament tel que visé à l'article 4, 1), du Règlement (UE) 2019/6 du Parlement et du Conseil du 11 décembre 2018 relatif aux médicaments vétérinaires et abrogeant la directive 2001/82/CE;

2°/4 "médicament homéopathique":

— un médicament homéopathique à usage humain tel que visé à l'article 1er, § 1er, 5), de la loi du 25 mars 1964 sur les médicaments à usage humain, ou

— un médicament vétérinaire homéopathique tel que visé à l'article 4, 10), du Règlement 2019/6 susmentionné;

2°/5 "médicament à base de plantes": un médicament à usage humain tel que visé à l'article 1er, § 1er, 6), de la loi du 25 mars 1964 sur les médicaments à usage humain;";

2° le 3° est remplacé comme suit:

"3° "préparation magistrale":

— un médicament à usage humain préparé en pharmacie conformément à une prescription médicale destinée à un patient déterminé, ou

— un médicament vétérinaire préparé en pharmacie conformément à une ordonnance vétérinaire pour un animal déterminé ou un petit groupe d'animaux;"