Rolnummer 6672
Arrest nr. 158/2021 van 18 november 2021

A R R E S T

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.

De Ministerraad, bijgestaan en vertegenwoordigd door Mr. S. Depré, Mr. E. de Lophem en Mr. T. Wouters, advocaten bij de balie te Brussel, heeft een memorie ingediend, de verzoekende partijen hebben een memorie van antwoord ingediend en de Ministerraad heeft ook een memorie van wederantwoord ingediend.

Bij beschikking van 7 februari 2018 heeft het Hof, na de rechters-verslaggevers A. Alen en J.-P. Moerman te hebben gehoord, beslist dat de zaak in staat van wijzen is, dat geen terechtzitting zal worden gehouden, tenzij een partij binnen zeven dagen na ontvangst van de kennisgeving van die beschikking een verzoek heeft ingediend om te worden gehoord, en dat, behoudens zulk een verzoek, de debatten zullen worden gesloten op 28 februari 2018 en de zaak in beraad zal worden genomen.

Ingevolge het verzoek van de verzoekende partijen om te worden gehoord, heeft het Hof bij beschikking van 1 maart 2018 de dag van de terechtzitting bepaald op 21 maart 2018.

Bij beschikking van 28 maart 2018 heeft het Hof de zaak verdaagd naar de terechtzitting van 25 april 2018.

Op de openbare terechtzitting van 25 april 2018 :

- zijn verschenen :

. Mr. D. Pattyn, voor de verzoekende partijen, en Patrick Van Assche, in eigen persoon;

. Mr. E. de Lophem, Mr. T. Wouters en Mr. G. Ryelandt, advocaat bij de balie te Brussel, *loco* Mr. S. Depré, voor de Ministerraad;

- hebben voorzitter A. Alen en rechter J.-P. Moerman verslag uitgebracht;

- zijn de voornoemde advocaten gehoord;

- is de zaak in beraad genomen.

Bij beschikking van 19 juli 2018 heeft het Hof de behandeling van de zaak *sine die* geschorst.

Bij beschikking van 21 april 2021 heeft het Hof, na de rechters-verslaggevers D. Pieters, ter vervanging van emeritus voorzitter A. Alen, en T. Giet, ter vervanging van rechter J.-P. Moerman, wettig verhinderd, te hebben gehoord, beslist :

- de debatten te heropenen,

- de partijen uit te nodigen, in een uiterlijk op 31 mei 2021 in te dienen aanvullende memorie, waarvan ze binnen dezelfde termijn een kopie laten toekomen aan de andere partijen, hun standpunt te laten kennen over de weerslag van het arrest van het Hof van Justitie van de Europese Unie van 6 oktober 2020 in de zaken nrs. C-511/18, C-512/18 en C-520/18 en van het arrest van het Grondwettelijk Hof nr. 57/2021 van 22 april 2021 op het onderhavige beroep tot vernietiging,

- dat geen terechtzitting zal worden gehouden, tenzij een partij binnen zeven dagen na ontvangst van de kennisgeving van die beschikking een verzoek heeft ingediend om te worden gehoord,

- dat, in geval van een dergelijk verzoek, de zaak zal worden behandeld op de terechtzitting van 16 juni 2021, op het tijdstip dat later door de voorzitter zal worden bepaald, en

- dat, behoudens zulk een verzoek, de debatten zullen worden gesloten op 16 juni 2021 en de zaak in beraad zal worden genomen.

Aanvullende memories zijn ingediend door :

- de verzoekende partijen;

- de Ministerraad, bijgestaan en vertegenwoordigd door Mr. S. Depré, Mr. E. de Lophem en Mr. G. Ryelandt.

Ingevolge het verzoek van de Ministerraad om te worden gehoord, heeft de voorzitter bij beschikking van 5 mei 2021 het tijdstip van de terechtzitting van 16 juni 2021 bepaald op 14.00 uur.

Op de openbare terechtzitting van 16 juni 2021 :

- zijn verschenen :

. Mr. D. Pattyn, voor de verzoekende partijen, en Patrick Van Assche, in eigen persoon;

. Mr. E. de Lophem en Mr. G. Ryelandt, tevens *loco* Mr. S. Depré, voor de Ministerraad;

- hebben de rechters-verslaggevers D. Pieters en J.-P. Moerman verslag uitgebracht;

- zijn de voornoemde partijen gehoord;

- is de zaak in beraad genomen.

De bepalingen van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof met betrekking tot de rechtspleging en het gebruik van de talen werden toegepast.

II. *In rechte*

- A -

Ten aanzien van de ontvankelijkheid van het beroep

A.1. De verzoekende partijen zetten uiteen dat zij als eindgebruikers van telefoniediensten aan de hand van vooraf betaalde kaarten worden geconfronteerd met een identificatieplicht. Het verwerken, bewaren en meedelen van de in de bestreden wet vermelde persoonsgegevens impliceert volgens hen een verregaande inmenging in hun persoonlijke levenssfeer, aangezien de verplichte identificatie van eindgebruikers van telefoniediensten het mogelijk maakt een verband te leggen tussen de verzoekende partijen en hun verkeers- en lokalisatiegegevens.

Bovendien voeren zij aan dat zij als gemeenteraadsleden in de gemeente Brecht een versterkt recht op vrije meningsuiting genieten, dat het recht op het verkrijgen en verspreiden van informatie omvat, onder meer aan de hand van anonieme telecommunicatie.

A.2.1. De Ministerraad merkt op dat verscheidene kritieken die de verzoekende partijen in het kader van het onderhavige beroep tot vernietiging formuleren, in werkelijkheid betrekking hebben op de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie ». Tegen die wet hebben dezelfde verzoekende partijen een beroep tot vernietiging ingediend, dat bij het Hof is ingeschreven onder het rolnummer 6601. In zoverre de kritieken van de verzoekende partijen in werkelijkheid betrekking hebben op die wet en niet op de bestreden wet, is het beroep tot vernietiging niet ontvankelijk *ratione temporis*.

A.2.2. De verzoekende partijen beklemtonen dat zij de ongrondwettigheid van de bestreden wet deels afleiden uit de gevolgen die zij heeft indien zij in samenhang wordt gelezen met de wet van 29 mei 2016. Bij de beoordeling van de grondwettigheid van de bestreden wet dient het Hof bijgevolg rekening te houden met de wet van 29 mei 2016, zelfs in zoverre het beroep tot vernietiging is gericht tegen de bestreden wet, in samenhang gelezen met de wet van 29 mei 2016.

Ten aanzien van het eerste middel

A.3.1. In hun eerste middel voeren de verzoekende partijen aan dat artikel 2 van de bestreden wet niet bestaanbaar is met 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 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 ».

In hun verzoekschrift voeren zij aan dat de machtiging aan de Koning om de technische en administratieve maatregelen te bepalen die worden opgelegd aan de verkoopkanalen van elektronische-communicatiediensten en aan de ondernemingen die een identificatiedienst verstrekken, niet voldoende nauwkeurig is omschreven, niet is beperkt tot de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgesteld en niet waarborgt dat de verzamelde identificatiegegevens en identificatiedocumenten pertinent en evenredig zijn in het licht van de doelstellingen waarvoor zij worden verwerkt.

A.3.2. De verzoekende partijen zetten uiteen dat het bij de bestreden bepaling gewijzigde artikel 127 van de wet van 13 juni 2005 « betreffende de elektronische communicatie » de Koning machtigt om de technische en administratieve maatregelen te bepalen die aan de aanbieders aan het publiek van telecommunicatiediensten worden opgelegd om de eindgebruiker te identificeren. Die bepaling viseert zowel de eigen winkels van de operatoren als alle andere verkoopkanalen, zoals supermarkten of nachtwinkels, al bewaren die laatste verkoopkanalen zelf geen identificatiegegevens of -documenten. De bestreden bepaling is eveneens van toepassing op de vooraf betaalde kaarten van buitenlandse operatoren die in België worden verkocht. Vanaf de inwerkingtreding van het uitvoeringsbesluit mogen nieuwe vooraf betaalde kaarten niet meer worden geactiveerd zonder identificatie van de eindgebruiker. De oude vooraf betaalde kaarten moeten binnen een termijn van zes

maanden na de inwerkingtreding van het uitvoeringsbesluit worden geïdentificeerd, op straffe van het afsluiten van de communicatie door de operator.

A.3.3. De verzoekende partijen wijzen in hun verzoekschrift op de samenhang tussen de bestreden bepaling en de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie ». Die wet legt een verplichting tot algemene en ongedifferentieerde bewaring op aan de aanbieders van telecommunicatiediensten. Zij dienen de identificatiegegevens, de verbindings- en lokalisatiegegevens en de communicatiegegevens van hun klanten te bewaren. Die gegevens omvatten niet de inhoud, maar wel de herkomst en de bestemming van de communicatie. De wet van 29 mei 2016 regelt de toegang tot de bewaarde gegevens en richt ook een gemeenschappelijke coördinatiecel van de aanbieders en operatoren op, die belast is met het verlenen van die toegang. De informatie die door de aanbieders van telecommunicatiediensten wordt verzameld op grond van de bestreden bepaling, dient ook te worden bewaard in het kader van de wet van 29 mei 2016.

A.3.4. De verwerking van persoonsgegevens die bestaat in het verzamelen van de identificatiegegevens bedoeld in de bestreden bepaling, beperkt volgens de verzoekende partijen het recht op eerbiediging van het privéleven. Hetzelfde geldt voor de bewaring van die gegevens en voor de toegang ertoe krachtens de wet van 29 mei 2016.

Volgens de verzoekende partijen vereist artikel 22, eerste lid, van de Grondwet dat een dergelijke beperking haar grondslag vindt in een formele wet. Een delegatie aan de Koning zou slechts mogelijk zijn 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. Ook het Hof van Justitie oordeelt in zijn arrest van 8 april 2014 (C-293/12 en C-594/12) dat het recht op eerbied voor het privéleven slechts bij formele wet kan worden beperkt.

A.3.5.1. De bestreden bepaling bevat volgens de verzoekende partijen een te verregaande delegatie aan de Koning, doordat zij Hem machtigt om de technische en administratieve maatregelen te bepalen die aan de aanbieders en operatoren, de verkoopkanalen van elektronische-communicatiediensten en de ondernemingen die een identificatiedienst verstrekken, worden opgelegd, onder andere om de eindgebruiker te identificeren. Daarbij voert de bestreden bepaling een vermoeden in krachtens hetwelk de geïdentificeerde persoon, behoudens tegenbewijs, wordt geacht zelf de elektronische-communicatiedienst te gebruiken.

De Commissie voor de bescherming van de persoonlijke levenssfeer (hierna : CBPL) uitte kritiek op het ontwerp dat tot de bestreden wet heeft geleid, aangezien de wetgever zou hebben nagelaten om enkele essentiële elementen van de bestreden regeling bij wet te regelen, namelijk de verantwoordelijke voor de verwerking, de bepaling wie toegang heeft tot de gegevens en het vaststellen van de bewaartermijn (advies nr. 54/2015 van 16 december 2015). Die kritiek werd vervolgens herhaald door de afdeling wetgeving van de Raad van State in haar advies bij de bestreden wet. Volgens de verzoekende partijen is de wetgever onvoldoende tegemoetgekomen aan die kritieken, doordat hij niet heeft bepaald welke identificatiegegevens dienen te worden verzameld, doordat hij niet heeft gepreciseerd welke identificatiedocumenten als bewijskrachtig kunnen worden aanvaard, en doordat hij geen criteria heeft bepaald om de delegatie aan de Koning te omkaderen met betrekking tot de differentiatie tussen de oude en de nieuwe vooraf betaalde kaarten.

A.3.5.2. Het soort informatie dat kan worden bewaard, is volgens de verzoekende partijen een essentieel element dat door de wetgever moet worden geregeld en dat niet aan de Koning kan worden gedelegeerd. De Koning beschikt op grond van de bestreden bepaling over een te grote discretionaire vrijheid inzake het regelen van het soort informatie dat wordt verzameld en bewaard, aangezien de bestreden bepaling niet verduidelijkt wat onder « identificatiegegevens en -documenten » dient te worden verstaan. Zo is niet duidelijk of het kan gaan om gegevens die betrekking hebben op de fysieke, fysiologische, psychische, economische, culturele of sociale identiteit van de eindgebruiker. Het gebrek aan afbakening laat de Koning toe om elk persoonsgegeven in aanmerking te nemen in het kader van de bestreden bepaling.

A.3.5.3. Ook de categorieën van personen over wie informatie kan worden ingewonnen, vormen een essentieel element dat niet aan de Koning kan worden gedelegeerd. De bestreden bepaling maakt slechts gewag van de « eindgebruiker ». Artikel 2, 13°, van de wet van 13 juni 2005 definieert een eindgebruiker als een gebruiker die geen openbaar elektronische-communicatienetwerk of openbare elektronische-communicatiediensten aanbiedt. Artikel 2, 12°, van dezelfde wet definieert een gebruiker als een natuurlijke of rechtspersoon die gebruik maakt van of verzoekt om een openbare elektronische-communicatiedienst. Aldus wordt aan de Koning een discretionaire vrijheid gegeven die Hem

toelaat om aan alle natuurlijke personen of rechtspersonen die gebruik maken van een elektronische-communicatienetwerk zonder er zelf een aan te bieden, een identificatieplicht op te leggen.

A.3.5.4. Ook de omstandigheden waaronder de gegevensverwerkingen kunnen gebeuren, de personen die het recht hebben om de opgeslagen informatie te raadplegen en de uiterste bewaartermijn van de gegevens zijn volgens de verzoekende partijen essentiële elementen. De bestreden bepaling beperkt zich in dat opzicht tot de vermelding dat de inlichtingen- en veiligheidsdiensten de medewerking kunnen vorderen van een bank of een financiële instelling om over te gaan tot het identificeren van de eindgebruiker, alsook tot de vaststelling dat de bewaring van de verzamelde gegevens geschiedt krachtens artikel 126, § 3, eerste lid, van de wet van 1 september 2016. In feite staat de bestreden bepaling de Koning toe om het toepassingsgebied en de inhoud van de wet van 29 mei 2016 aanzienlijk uit te breiden.

A.3.5.5. Tot slot maken ook de sancties bij niet-naleving van de identificatieplicht een essentieel element uit. Nochtans verbiedt de bestreden bepaling de aanbieders om nog elektronische-communicatiediensten aan te bieden indien zij niet voldoen aan de technische en administratieve maatregelen die de Koning bepaalt. Zij dienen bovendien de elektronische-communicatiedienst af te sluiten van eindgebruikers die niet aan de door de Koning bepaalde verplichtingen voldoen. Die sancties maken een ernstige aantasting van het recht op vrije meningsuiting van de eindgebruikers uit, zodat de inhoud van de gesanctioneerde verplichtingen niet aan de Koning mag worden overgelaten.

A.3.6. Meer algemeen waarborgt de bestreden bepaling volgens de verzoekende partijen niet dat de door de Koning uitgewerkte regeling ter zake dienend en niet overmatig is, in het licht van de doeleinden waarvoor de door de Koning opgelijste persoonsgegevens worden verwerkt.

A.4.1. De Ministerraad beklemtoont dat grondwetsbepalingen die een bevoegdheid voorbehouden aan de wetgever, geen absoluut delegatieverbod instellen. Het is de wetgever toegelaten een nauwkeurig afgelijnde bevoegdheid aan de Koning te delegeren voor zover hij de essentiële elementen van die materie zelf regelt.

In dat opzicht wijst de Ministerraad erop dat de bestreden bepaling amper delegaties aan de Koning bevat. Alleen artikel 127, § 3, tweede lid, van de wet van 1 september 2016 draagt aan de Koning de bevoegdheid op om het begrip « niet-geïdentificeerde eindgebruiker » te bepalen. Die delegatie werd door de verzoekende partijen niet bekritiseerd. De overige door de verzoekende partijen bestreden delegaties waren reeds in de wet van 13 juni 2005 vervat vooraleer zij werd gewijzigd bij de wet van 1 september 2016. In die mate is het eerste middel bijgevolg niet ontvankelijk.

De door de verzoekende partijen vermelde adviezen van de CBPL en van de afdeling wetgeving van de Raad van State zijn overigens niet relevant, aangezien de wetgever die adviezen heeft geïmplementeerd door in de bestreden bepaling de vereiste essentiële elementen op te nemen.

Daarnaast merkt de Ministerraad op dat het niet de wet van 1 september 2016 is die de identificatie van gebruikers van vooraf betaalde kaarten mogelijk maakt. Dat principe was reeds ingeschreven in artikel 127, § 3, eerste lid, van de wet van 13 juni 2005 en werd door de bestreden bepaling niet gewijzigd.

A.4.2. Met betrekking tot het soort informatie dat kan worden bewaard, argumenteert de Ministerraad dat de wetgever geen delegatie aan de Koning geeft om te bepalen wat wordt bedoeld met « identificatiegegevens of -documenten ». Die begrippen werden ingevoegd in artikel 127, § 1, achtste lid, van de wet van 13 juni 2005 zonder dat de Koning wordt gemachtigd om die begrippen nader te definiëren. De afdeling wetgeving van de Raad van State heeft hieromtrent overigens geen opmerkingen geformuleerd.

Het enige essentiële element dat bij wet diende te worden geregeld, is het principe van de identificatie zelf. De methode, de gegevens en de documenten die daarbij betrokken zijn, vormen geen essentiële elementen van de bestreden beperking van het recht op eerbiediging van het privé- en gezinsleven, maar zijn slechts modaliteiten ervan.

Indien zou blijken dat de Koning toch identificatiegegevens en -documenten opneemt die niet verenigbaar zijn met de vereisten van de eerbiediging van de persoonlijke levenssfeer, kan het betrokken koninklijk besluit worden bestreden bij de afdeling bestuursrechtspraak van de Raad van State.

A.4.3. Ook met betrekking tot de categorieën van personen over wie informatie kan worden ingewonnen, argumenteert de Ministerraad dat zij niet het voorwerp uitmaken van de bestreden bepaling, maar reeds in artikel 127, § 1, 2°, van de wet van 13 juni 2005 werden geregeld vóór de wijziging ervan bij de bestreden wet.

Daarnaast is het uitdrukkelijk de bedoeling van de wetgever om een identificatieverplichting op te leggen aan alle eindgebruikers in de zin van artikel 2, 13°, van de wet van 13 juni 2005, zodat het niet nodig is om hieromtrent een delegatie aan de Koning te geven.

A.4.4. Ook de omstandigheden waaronder de gegevensverwerkingen kunnen gebeuren, de personen die het recht hebben om de opgeslagen informatie te raadplegen en de uiterste bewaartermijn van de gegevens, werden reeds in artikel 127 van de wet van 13 juni 2005 geregeld vooraleer die bepaling werd gewijzigd bij de bestreden bepaling. Die bepaling verwijst overigens naar artikel 126 van dezelfde wet, dat nauwkeurig regelt welke autoriteiten toegang hebben tot de bewaarde gegevens en binnen welke termijn dat dient te gebeuren.

A.4.5. Ook de sancties bij niet-naleving van de identificatieplicht worden volledig bepaald in artikel 127, §§ 4 en 5, van de wet van 13 juni 2005, zodat er geen ruimte bestaat voor een delegatie aan de Koning.

A.5.1. De verzoekende partijen wijzen erop dat, wanneer de wetgever opnieuw normerend optreedt in een bepaalde materie, en daarbij een bestaande machtiging aan de Koning uitbreidt, het Hof bevoegd is om kennis te nemen van een beroep tegen die uitbreiding. De bestreden bepaling houdt een aanzienlijke verstrenging in van artikel 127 van de wet van 13 juni 2005, aangezien zij de facultatieve identificatie van de eindgebruiker heeft veranderd in een verplichte identificatie. Zij doet dit aan de hand van verscheidene delegaties aan de Koning. Bovendien voert de bestreden bepaling een verbod op de verkoop van nieuwe vooraf betaalde kaarten in en verplicht zij tot de buitenwerkingstelling van oude vooraf betaalde kaarten waarvan de eigenaar zich niet binnen de door de Koning bepaalde termijn identificeert.

Overigens heeft de Koning krachtens de artikelen 37 en 108 van de Grondwet geen uitdrukkelijke machtiging nodig om de verordeningen te maken en de besluiten te nemen die nodig zijn voor de uitvoering van de wetten. De bestreden bepaling verleent bijgevolg een impliciete machtiging aan de Koning om regelgevend op te treden in een materie die door artikel 22, eerste lid, van de Grondwet aan de wetgever wordt voorbehouden.

Niets verhindert dat de bestreden bepaling de Koning uitdrukkelijk machtigt om de technische en administratieve maatregelen te bepalen die aan de verkoopkanalen van elektronische-communicatiediensten en aan de ondernemingen die een identificatiedienst verstrekken, worden opgelegd, onder andere wat de identificatie van de eindgebruiker betreft. Evenmin neemt het voorgaande weg dat de verzamelde identificatiegegevens en -documenten worden bewaard overeenkomstig artikel 126, § 3, eerste lid, van de wet van 13 juni 2005, noch dat artikel 127, §§ 4 en 5, van dezelfde wet de sancties bepalen die worden opgelegd aan operatoren en aanbieders van elektronische-communicatiediensten die niet aan de door de Koning opgelegde technische en administratieve maatregelen voldoen.

Tot slot wijzen de verzoekende partijen erop dat de aanhef van 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 », preciseert dat dit koninklijk besluit zijn grondslag vindt in artikel 127, § 1, van de wet van 13 juni 2005, zoals laatst gewijzigd bij de wet van 1 september 2016.

A.5.2.1. Met betrekking tot het soort informatie dat kan worden bewaard, blijkt dat de bestreden bepaling essentiële begrippen zoals de « identificatiegegevens of -documenten » niet omschrijft, terwijl zowel de CBPL als de afdeling wetgeving van de Raad van State daarop hadden aangedrongen. Voor het overige blijkt uit het arrest *Rotaru t. Roemenië* van 4 mei 2000 van het Europees Hof voor de Rechten van de Mens dat het soort informatie dat wordt verzameld, wel degelijk een essentieel element is dat door de wetgever dient te worden geregeld.

A.5.2.2. Met betrekking tot de categorieën van personen over wie informatie kan worden ingewonnen, herhalen de verzoekende partijen dat de identificatie van eindgebruikers van vooraf betaalde kaarten vroeger facultatief was en dat de bestreden bepaling die identificatie verplicht heeft gesteld. Zij breidt daarnaast de machtiging aan de Koning om de technische en administratieve maatregelen te bepalen om de eindgebruiker te identificeren, uit tot de verkoopkanalen van elektronische-communicatiediensten en de ondernemingen die een identificatiedienst verstrekken.

A.5.2.3. Met betrekking tot de omstandigheden waaronder de gegevensverwerking kan plaatsvinden, de personen die het recht hebben de opgeslagen informatie te raadplegen en de uiterste bewaartermijn van de

gegevens, zijn de verzoekende partijen van oordeel dat de argumentatie van de Ministerraad naast de kwestie is. De Koning beschikt over een te ruime appreciatiebevoegdheid om te bepalen welke identificatiegegevens of -documenten moeten worden verzameld en welke categorieën van eindgebruikers aan de identificatieplicht worden onderworpen.

A.5.2.4. Met betrekking tot de gevolgen van de niet-naleving van de identificatieplicht wijzen de verzoekende partijen erop dat de Koning kan bepalen dat zelfs de meest geringe inbreuk aanleiding geeft tot het niet-aanbieden of het afsluiten van elektronische-communicatiediensten. Een dergelijk stelsel van sanctionering is onevenredig met de nagestreefde doelstelling.

A.6. De Ministerraad stelt vast dat de verzoekende partijen niet uit de bestreden bepaling, maar uit het door de bestreden bepaling niet gewijzigde artikel 126 van de wet van 13 juni 2005 en uit het verslag aan de Koning bij het koninklijk besluit van 27 november 2016 afleiden dat de wetgever een delegatie aan de Koning heeft gegeven. Dergelijke gegevens kunnen evenwel niet in aanmerking worden genomen om de grondwettigheid van de bestreden bepaling te beoordelen.

A.7. In hun aanvullende memorie voeren de verzoekende partijen aan dat de vernietiging van artikel 126 van de wet van 13 juni 2005 bij het arrest van het Hof nr. 57/2021 van 22 april 2021 de wettelijke grondslag van de bestreden privacybeperking nog onduidelijker maakt. De bestreden bepaling machtigt de Koning immers om de bestreden gegevensverwerking te regelen met het oog op een bewaarplicht die door het Hof is vernietigd. Als gevolg van die vernietiging is bewaring van de persoonsgegevens bedoeld in de bestreden bepaling aan geen enkele voorwaarde meer onderworpen. Geen enkele wetsbepaling regelt thans op welke gegevens de bewaring slaat, wie de bij de gegevensverwerking betrokken personen zijn en welke de voorwaarden en doeleinden van de verwerking zijn. Bijgevolg is ook de wettelijke grondslag van de initiële gegevensverwerking bedoeld in de bestreden bepaling aangetast.

A.8. De Ministerraad merkt in zijn aanvullende memorie op dat een nieuwe dataretentieregeling die voldoet aan de in het arrest van het Hof nr. 57/2021 vermelde vereisten thans in voorbereiding is. De wettelijke grondslag voor de gegevensverwerking zal dus spoedig worden hersteld.

Ten aanzien van het tweede middel

A.9. In hun tweede middel voeren de verzoekende partijen aan dat de artikelen 2 en 3 van de bestreden wet niet bestaanbaar zijn met 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 en 52 van het Handvest van de grondrechten van de Europese Unie, 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 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 », 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) ». Het middel valt uiteen in drie onderdelen.

Het eerste onderdeel van het tweede middel

A.10. In het eerste onderdeel van het tweede middel klagen de verzoekende partijen aan dat de door de bestreden wet ingevoerde algemene en ongedifferentieerde identificatieplicht voor alle eindgebruikers van alle elektronische-communicatiediensten een ongerechtvaardigde inmenging in het recht op bescherming van de persoonlijke levenssfeer vormt.

A.11.1. De verzoekende partijen zetten uiteen dat artikel 127 van de wet van 13 juni 2005, zoals gewijzigd bij artikel 2 van de bestreden wet, ertoe strekt de anonimiteit van de vooraf betaalde kaart van de mobiele operatoren af te schaffen. De verkoop van nieuwe anonieme vooraf betaalde kaarten wordt verboden, terwijl de eindgebruikers van oude vooraf betaalde kaarten verplicht worden geïdentificeerd. Die verplichting moet in samenhang worden gelezen met de wet van 29 mei 2016, die een plicht tot algemene en ongedifferentieerde bewaring oplegt aan de aanbieders aan het publiek van internet- en telefoniediensten om de eindgebruiker of de

abonnee te identificeren en te lokaliseren. De gegevens die worden verzameld krachtens de bestreden bepalingen, moeten immers worden bewaard en meegedeeld volgens de procedures vastgelegd in de wet van 29 mei 2016.

A.11.2.1. Volgens de verzoekende partijen is de richtlijn 2002/58/EG van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare communicatienetwerken in de Europese Unie. De identificatiegegevens die krachtens de bestreden wet worden verzameld, vormen persoonsgegevens in de zin van die richtlijn. Uit de rechtspraak van het Hof van Justitie van de Europese Unie blijkt dat zulks ook geldt voor de verwerking en bewaring van communicatiegegevens met het oog op de nationale veiligheid, de landsverdediging en het voorkomen en vervolgen van strafbare feiten. Bijgevolg valt de bestreden wet binnen de werkingssfeer van het Europees Unierecht.

A.11.2.2. De bestreden bepalingen, alsook de bewaring van de verzamelde identificatiegegevens krachtens de wet van 29 mei 2016, maken bovendien een beperking uit van het recht op eerbiediging van het privé- en gezinsleven, zoals overigens blijkt uit het arrest van het Hof nr. 108/2016 van 14 juli 2016.

A.11.2.3. Een dergelijke beperking kan blijkens de rechtspraak van het Hof van Justitie van de Europese Unie slechts worden gerechtvaardigd in zoverre er een strikt rechterlijk toezicht bestaat op de naleving van het evenredigheidsbeginsel. Die evenredigheidstoets vereist dat wordt nagegaan of het nagestreefde doel kan worden verwezenlijkt door de bewaring van de gegevens, dat de uitzonderingen op de bescherming van de persoonsgegevens binnen de grenzen van het strikt noodzakelijke blijven en dat de verzameling van persoonsgegevens geschiedt in het kader van duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel. Die regels moeten objectieve criteria bevatten die de toegang van de bevoegde nationale autoriteiten tot de persoonsgegevens begrenzen. Ook moet de toepassing ervan onderworpen zijn aan een voorafgaande rechterlijke controle of een voorafgaande controle door een onafhankelijke administratieve instantie. Bovendien moet de termijn gedurende welke de gegevens worden bewaard, aangepast zijn aan het doel waarvoor de gegevens worden bewaard. Tot slot moeten de verzamelde gegevens worden beveiligd tegen onrechtmatige toegang.

A.11.3.1. In de parlementaire voorbereiding van de bestreden bepalingen wordt gepreciseerd dat de afschaffing van de anonimiteit van de vooraf betaalde kaarten tegemoetkomt aan een vraag van de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten en de nooddiensten. Aangezien de vooraf betaalde kaarten wijd verspreid zijn in criminele kringen, is de identificatie van de eindgebruiker cruciaal in de strijd tegen het terrorisme en in het opsporen en vervolgen van zware criminele feiten. Elke andere techniek om de eindgebruiker te identificeren, zou overigens een grotere inmenging in het privé- en gezinsleven inhouden dan de loutere toegang tot vooraf verzamelde gegevens en documenten. Overigens zijn houders van een telefonieabonnement niet anoniem, en zijn het alleen de houders van vooraf betaalde telefoonkaarten die tot op heden niet kunnen worden geïdentificeerd. De anonimiteit van de vooraf betaalde kaarten was trouwens steeds opgevat als een tijdelijke maatregel om de intrede van de gsm op de Belgische markt te ondersteunen.

A.11.3.2. De verzoekende partijen zijn van mening dat enkel de strijd tegen de zware misdaad en tegen het terrorisme de bestreden identificatieplicht kan rechtvaardigen. De overige in de parlementaire voorbereiding vermelde doelstellingen mogen daarentegen niet in aanmerking worden genomen in het kader van de beperking van een fundamenteel recht als de eerbied voor het privé- en gezinsleven. Ook uit de rechtspraak van het Hof van Justitie met betrekking tot artikel 15, lid 1, van de richtlijn 2002/58/EG blijkt volgens de verzoekende partijen dat de mogelijkheid die deze bepaling biedt om persoonsgegevens te verwerken met het oog op de nationale veiligheid, enkel mag worden aangewend voor de doelstellingen die limitatief in die bepaling worden opgesomd. Uit die rechtspraak zou ook blijken dat die doelstelling niet mag worden aangewend om van de opslag van persoonsgegevens de regel te maken. Hoewel de strijd tegen de zware misdaad en het terrorisme in grote mate afhangt van het gebruik van moderne technologieën, mag een dergelijke doelstelling immers niet leiden tot een nationale regeling die voorziet in een algemene en ongedifferentieerde bewaring van alle verkeersgegevens en alle lokalisatiegegevens.

A.11.4.1. De bestreden identificatieplicht is niet evenredig met de doelstelling om de zware misdaad en het terrorisme te verwezenlijken. Ten eerste is zij niet geschikt om die doelstelling te bereiken, aangezien zij niet verbiedt om een vooraf betaalde kaart aan een derde over te dragen. Overigens kan een gsm-toestel dat gebruik maakt van een vooraf betaalde kaart, ook worden gestolen. In dergelijke gevallen leiden de bestreden bepalingen veelal tot de identificatie van een persoon die niets met het onderzochte misdrijf te maken heeft, terwijl de dader niet wordt geïdentificeerd. Ten tweede verbieden de bestreden bepalingen niet dat in het buitenland aangekochte anonieme vooraf betaalde kaarten op grond van internationale *roaming* in België worden gebruikt. Ten derde

bestaan er verschillende vormen van elektronische communicatie die niet door de bestreden bepalingen worden geviseerd en die eveneens kunnen worden gebruikt in het kader van criminele en terroristische activiteiten.

A.11.4.2. Daarnaast ontbreken volgens de verzoekende partijen duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de bestreden wet. Zij bepaalt immers niet welke persoonsgegevens mogen worden ingezameld, welke categorieën van personen moeten worden geïdentificeerd, hoe en hoe lang de gegevens worden bewaard en wie er toegang toe heeft.

Bijgevolg valt ook onmogelijk vast te stellen of de verzamelde gegevens strikt noodzakelijk zijn op grond van de doelstelling van een efficiënte bestrijding van het terrorisme en de zware misdaad.

A.11.4.3. Ook de toegang tot de verzamelde gegevens en de bescherming en de beveiliging van die gegevens worden onvoldoende geregeld. Duidelijk is enkel dat die gegevens worden bewaard krachtens artikel 126 van de wet van 13 juni 2005, zoals laatst gewijzigd bij de wet van 29 mei 2016. Uit het beroep tot vernietiging dat de verzoekende partijen hebben ingesteld tegen die wet en dat bij het Hof is ingeschreven onder het rolnummer 6601, blijkt dat die bepaling geenszins volstaat, aangezien zij de vertrouwelijkheid van de gegevens niet regelt.

A.12.1. De Ministerraad is van oordeel dat de verwijzing naar de richtlijnen 95/46/EG en 2002/58/EG gebaseerd is op een onjuiste analyse van de draagwijdte van de bestreden wet. Die wet heeft immers geen betrekking op de communicatie-, lokalisatie- of verkeersgegevens in de zin van die richtlijnen, maar enkel op de identificatie van de houder van een vooraf betaalde kaart op het ogenblik waarop hij die kaart koopt. Er wordt geen enkel ander persoonsgegeven verwerkt dan de identiteit van de koper.

A.12.2. De verzoekende partijen tonen nergens aan dat het recht op bescherming van de persoonlijke levenssfeer ook een recht op anonimiteit zou inhouden. In die zin moet een onderscheid worden gemaakt tussen de inhoud van de bestreden wet en de inhoud van de wet van 29 mei 2016, die wel een verwerking van persoonsgegevens regelt. De bestreden bepalingen regelen niet hoe een vooraf betaalde kaart al dan niet mag worden gebruikt, maar regelen enkel de identificatie van de eindgebruiker.

A.12.3. Die identificatie is noodzakelijk in het kader van een efficiënte strijd tegen de zware misdaad en het terrorisme. Alsmaar meer Europese landen voeren een soortgelijke regeling in. Indien zou blijken dat die maatregel niet perfect is en door handige criminelen kan worden omzeild, moet die maatregel worden verstrengd; hieruit kan evenwel niet worden afgeleid dat de bestreden bepalingen in hun huidige vorm niet noodzakelijk zouden zijn. Veel van de lacunes die de verzoekende partijen opmerken, worden overigens uitdrukkelijk geregeld in andere wettelijke en reglementaire bepalingen. Zo regelt het koninklijk besluit van 27 november 2016 de situatie van de verkoop of de diefstal van vooraf betaalde kaarten. Het gevaar van internationale *roaming* wordt op zijn beurt opgevangen door artikel 6*ter* van de verordening (EU) 2015/2120 van het Europees Parlement en de Raad van 25 november 2015 « tot vaststelling van maatregelen betreffende open-internettoegang en tot wijziging van Richtlijn 2002/22/EC inzake de universele dienst en gebruiksrechten met betrekking tot elektronische-communicatienetwerken en –diensten en Verordening (EU) nr. 531/2012 betreffende roaming op openbare mobielecommunicatienetwerken binnen de Unie ».

De verzoekende partijen zetten overigens niet uiteen waarom ter zake een verschil in behandeling tussen vooraf betaalde kaarten en abonnementen zou moeten worden gehandhaafd.

A.13.1. De verzoekende partijen antwoorden dat krachtens artikel 2, a), van de richtlijn 95/46/EG iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon een persoonsgegeven is. De gegevens die krachtens de bestreden bepalingen vereist zijn om de eindgebruiker te identificeren, maken dus persoonsgegevens uit. Uit de rechtspraak van het Hof van Justitie van de Europese Unie blijkt overigens dat de activiteiten van aanbieders van elektronische-communicatiediensten binnen de werkingssfeer van de richtlijn 2002/58/EG vallen.

De omstandigheid dat de bestreden wet alleen betrekking heeft op identificatiegegevens, neemt niet weg dat die gegevens dienen te worden verwerkt op grond van de wet van 29 mei 2016. De bestreden wet heeft als gevolg dat ook de loutere identificatiegegevens moeten worden bewaard door de aanbieders en de operatoren en dat zij worden verwerkt op een manier die overheden toelaat om hen te gebruiken.

A.13.2. Volgens de verzoekende partijen blijkt uit wetenschappelijk onderzoek en uit persartikels dat de identificatieplicht niet noodzakelijk en niet doeltreffend is in de strijd tegen de zware misdaad en tegen het

terrorisme. Een maatregel die niet doeltreffend kan zijn, is per definitie evenmin evenredig met de nagestreefde doelstelling.

De wil om het beweerde verschil in behandeling tussen eindgebruikers van vooraf betaalde kaarten en houders van een telefonieabonnement af te schaffen, kan de bestreden maatregel niet verantwoorden, aangezien dit geen verband houdt met de nationale veiligheid, het economisch welzijn van het land, de strijd tegen de zware misdaad of de volksgezondheid.

A.13.3. Het door de Ministerraad vermelde koninklijk besluit van 27 november 2016 neemt niet weg dat de daadwerkelijke gebruiker van een vooraf betaalde kaart niet kan worden geïdentificeerd aan de hand van de identificatiegegevens van de koper. Hieraan voegen de verzoekende partijen toe dat rechtspersonen eenvoudig de identificatieplicht kunnen omzeilen.

Ook de door de Ministerraad vermelde verordening (EU) 2015/2120 verhindert niet dat met internationale *roaming* een in het buitenland aangekochte vooraf betaalde kaart de bestreden bepalingen kan omzeilen. Een misbruik van internationale *roaming* wordt op grond van die verordening overigens niet gesanctioneerd met het blokkeren van die kaart, maar slechts met het betalen van een toeslag. De georganiseerde misdaad of terroristische groeperingen zullen zich niet door een dergelijke toeslag laten afschrikken.

A.13.4. De bestreden bepalingen hebben bijgevolg vooral nadelige gevolgen voor particulieren, terwijl rechtspersonen, criminele organisaties en terroristische organisaties de werking ervan vlot kunnen omzeilen. Aldus dreigen de bestreden bepalingen met name kwetsbare personen te raken, die zich niet eenvoudig kunnen identificeren, zoals vreemdelingen.

A.14. De Ministerraad beklemtoont dat personen die moeilijkheden ondervinden om zich te identificeren, niet onmiddellijk zullen worden afgesloten. Eerst zal opnieuw worden geprobeerd om hen te identificeren. De documenten waarover geregistreerde vreemdelingen beschikken, voldoen overigens aan de identificatiestandaarden.

A.15. De verzoekende partijen wijzen er in hun aanvullende memorie op dat het Hof van Justitie bij zijn arrest van 6 oktober 2020 in zake *La Quadrature du Net e.a.* (C-511/18), heeft geoordeeld dat er slechts mag worden voorzien in de algemene en ongedifferentieerde bewaring van identificatiegegevens als dat gebeurt op grond van « duidelijke en nauwkeurige regels [die] 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 ». Dat duidelijke en nauwkeurige rechtskader is na de vernietiging van de dataretentieregeling bij het arrest nr. 57/2021 niet meer voorhanden. Aangezien ook de bepalingen over de Coördinatiecel zijn vernietigd, is de vertrouwelijkheid van de bewaarde identiteitsgegevens niet gewaarborgd.

A.16.1. De Ministerraad wijst in zijn aanvullende memorie op het onderscheid tussen de vernietigde dataretentieregeling en de thans bestreden bepaling. De bestreden bepaling heeft geen betrekking op verkeers- en lokalisatiegegevens. De identificatiegegevens van de houder van een vooraf betaalde kaart worden niet verwerkt als « verkeersgegevens » in de zin van artikel 2, 6°, van de wet van 13 juni 2005, aangezien hij geen factuur ontvangt. Van de eindgebruiker van een vooraf betaalde kaart worden dus slechts identificatiegegevens verwerkt. In geen geval worden zijn gegevens verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk. De bestreden wet heeft geen betrekking op de toegang tot de opgeslagen gegevens : die toegang wordt geregeld in de organieke wetgeving van de organen die toegang tot die gegevens mogen hebben. Die wetgeving wordt thans niet bestreden.

A.16.2. De Ministerraad wijst in zijn aanvullende memorie tevens erop dat het Hof van Justitie in zijn arrest van 6 oktober 2020 in zake *La Quadrature du Net e.a.* (C-511/18), heeft geoordeeld dat artikel 15, lid 1, van de richtlijn 2002/58/EG zich niet verzet tegen een algemene en ongedifferentieerde bewaring van loutere identificatiegegevens. Aan de hand van de burgerlijke identiteit kunnen immers noch de datum, het tijdstip, de duur en de ontvangers van de communicatie worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Een dergelijke inmenging in het privéleven werd door het Hof van Justitie niet als ernstig beschouwd.

Het tweede onderdeel van het tweede middel

A.17. In het tweede onderdeel van het tweede middel klagen de verzoekende partijen aan dat de door de bestreden bepalingen ingevoerde identificatieplicht de uitoefening van het vrij verkeer van diensten belemmert, terwijl die beperking niet geschikt is in het kader van de bestrijding van de zware misdaad en het terrorisme en verder gaat dan noodzakelijk is om die doelstelling te bereiken.

A.18.1.1. Volgens de verzoekende partijen verbieden de artikelen 56 en 57 van het Verdrag betreffende de werking van de Europese Unie elke nationale maatregel die wordt opgelegd aan een dienstverrichter die in een andere lidstaat is gevestigd en aldaar rechtmatig diensten verricht, en die hem beperkt in het aanbieden van soortgelijke diensten op het nationale grondgebied. Dergelijke beperkingen zijn slechts toelaatbaar indien zij een doel van algemeen belang nastreven, geschikt zijn om het beoogde doel te bereiken en niet verder gaan dan wat noodzakelijk is om het gestelde doel te bereiken. Een nationale wettelijke regeling die de vrijheid van dienstverrichting beperkt om dwingende redenen van algemeen belang, is overigens slechts geschikt om de gestelde doelstelling te verwezenlijken wanneer die verwezenlijking op samenhangende en stelselmatige wijze wordt nagestreefd.

A.18.1.2. De verzoekende partijen wijzen erop dat de wet van 13 juni 2005 van toepassing is op eenieder die gewoonlijk tegen vergoeding een dienst aanbiedt die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische-communicatienetwerken. Dergelijke diensten vallen onder het toepassingsgebied van de artikelen 56 en 57 van het Verdrag betreffende de werking van de Europese Unie. De bestreden bepalingen zijn overigens zonder onderscheid van toepassing op zowel de binnenlandse als de buitenlandse operatoren die in België vooraf betaalde kaarten aanbieden. Het volstaat dat die kaart is verbonden aan een Belgisch telefoonnummer of een Belgische IMSI (International Mobile Subscriber Identity), of dat de vooraf betaalde kaart wordt verkocht in België.

A.18.2. De identificatieplicht houdt in dat alle dienstverrichters die onder het toepassingsgebied van de bestreden bepalingen vallen, moeten overgaan tot de identificatie van de eindgebruikers en dat zij de technische en administratieve maatregelen die door de Koning worden bepaald, moeten naleven. Het is hun verboden elektronische-communicatiediensten aan te bieden die niet aan die voorwaarden voldoen. Zij moeten bovendien de oude vooraf betaalde kaarten van de eindgebruikers die weigeren zich te identificeren, afsluiten, en zij moeten weigeren om nieuwe vooraf betaalde kaarten te activeren indien de koper weigert zich te identificeren. Die maatregelen belemmeren het vrij verkeer van diensten of maken het minstens minder beschikbaar.

A.18.3. Uit de uiteenzetting van het eerste onderdeel van het tweede middel leiden de verzoekende partijen af dat de bestreden bepalingen niet geschikt zijn in het licht van de strijd tegen de zware misdaad en het terrorisme. Dit is des te meer het geval nu de bestreden identificatieplicht niet het voorwerp uitmaakt van geharmoniseerde wetgeving op het niveau van de Europese Unie. Belgische gebruikers kunnen bijgevolg op basis van internationale *roaming* een vooraf betaalde kaart aankopen in het buitenland en zo anoniem blijven, maar niettemin wordt het buitenlandse operatoren moeilijker gemaakt om hun diensten in België aan te bieden.

A.19.1. Volgens de Ministerraad beperken de bestreden bepalingen geenszins het vrij verkeer van diensten. Niet elke wetskrachtige norm die een verplichting oplegt aan ondernemingen, heeft een restrictief effect op het vrij verkeer van diensten. De bestreden bepalingen leggen louter administratieve verplichtingen op aan de dienstverleners van elektronische-communicatiediensten. Die verplichtingen bedreigen op geen enkele manier de activiteiten van de buitenlandse operatoren op Belgisch grondgebied.

A.19.2. In ondergeschikte orde voert de Ministerraad aan dat de bestreden beperking van het vrij verkeer van diensten geschikt is in het licht van de bestrijding van de zware misdaad en het terrorisme en in een redelijke verhouding van evenredigheid tot die doelstelling staat. Een dergelijke doelstelling vormt een dwingende reden van algemeen belang die een beperking van het vrij verkeer van diensten toelaat. De identificatie van misdadigers en terroristen aan de hand van hun dataverkeer is noodzakelijk en adequaat in het licht van een efficiënte bestrijding van die fenomenen. De loutere omstandigheid dat hieromtrent geen geharmoniseerde wetgeving op Europees niveau bestaat, volstaat niet om de pertinentie van de bestreden maatregelen in het licht van de nagestreefde doelstelling in twijfel te trekken.

De Ministerraad beklemtoont dat het Hof van Justitie over het algemeen de beperkingen op het vrij verkeer van diensten die bestaan in administratieve maatregelen, aanvaardt. Zo aanvaardde het reeds dat ondernemingen die uitzendings- en digitale televisiesignalen commercialiseren, zich moeten inschrijven in een nationaal register.

Ook aanvaardde het dat bouwondernemingen sociale en arbeidsdocumenten moeten bijhouden in de lidstaat van ontvangst.

A.20.1. De verzoekende partijen zijn van mening dat, gelet op de algemene formulering van artikel 56 van het Verdrag betreffende de werking van de Europese Unie, ook louter administratieve verplichtingen een belemmering van het vrij verkeer van diensten vormen. De opgelegde verplichting houdt immers bijkomende administratieve en financiële lasten in die de dienstverrichters kunnen afschrikken om in België elektronische-communicatiediensten aan te bieden. Die administratieve last wordt overigens erkend in de parlementaire voorbereiding.

A.20.2. De minister van Justitie heeft in de plenaire vergadering van 18 juni 2015 trouwens aangegeven dat hij een studie heeft besteld over de afschaffing van anonieme vooraf betaalde kaarten, omdat de operatoren vreesden dat die maatregel de administratieve rompslomp zou verhogen. Die studie, die door de Ministerraad niet wordt overgezonden, lijkt relevant in het licht van de beoordeling van de belemmering van het vrij verkeer van diensten, omdat hieruit de nodige gegevens kunnen blijken met betrekking tot de geschiktheid en de evenredigheid van de bestreden bepalingen. Daarom vragen de verzoekende partijen dat het Hof overeenkomstig artikel 91, 2°, van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof zou beslissen dat de Ministerraad die studie ter beschikking moet stellen.

A.21. De Ministerraad stelt vast dat de verzoekende partijen geen enkel element aanhalen waaruit blijkt dat de bestreden bepalingen een dergelijk zware administratieve last opleggen dat zij buitenlandse operatoren zouden afschrikken om in België een elektronische-communicatiedienst aan te bieden.

Overigens blijkt uit artikel 130 van de wet van 13 juni 2005 dat een beperkte anonimiteit mogelijk blijft. Krachtens die bepaling moeten de operatoren het immers gratis mogelijk maken dat het oproepnummer van de eindgebruiker anoniem blijft bij de ontvanger van de communicatie.

A.22. In hun aanvullende memorie voeren de verzoekende partijen aan dat het arrest van het Hof nr. 57/2021 van 22 april 2021 niet relevant is voor de beoordeling van het tweede onderdeel van het tweede middel.

Het derde onderdeel van het tweede middel

A.23. In het derde onderdeel van het tweede middel klagen de verzoekende partijen aan dat de door de bestreden bepalingen ingevoerde identificatieplicht een ongerechtvaardigde beperking vormt van de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken en van het journalistieke bronnengeheim.

A.24. De vrijheid van meningsuiting omvat de vrijheid om inlichtingen en denkbeelden van welke aard ook op te sporen, te ontvangen en door te geven, ongeacht grenzen, hetzij mondeling, hetzij in geschreven of gedrukte vorm, in de vorm van kunst, of met behulp van andere media naar keuze.

Aangezien de bestreden bepalingen een algemene en ongedifferentieerde identificatieplicht instellen voor alle eindgebruikers van elektronische-communicatiediensten, beperkt zij de vrijheid van meningsuiting. Uit de rechtspraak van het Hof van Justitie blijkt immers dat de bewaarplicht van communicatiegegevens van dien aard is dat de wijze waarop de gebruikers van elektronische-communicatiediensten hun vrijheid van meningsuiting gebruiken, wordt beïnvloed.

De verwerking, krachtens de wet van 29 mei 2016, van de identificatiegegevens bedoeld in de bestreden bepalingen, maakt het mogelijk om van elke burger een persoonlijkheidsprofiel op te stellen en zijn bewegingen te volgen. Klokkenluiders zullen aldus worden geremd in hun contacten met politici en met journalisten om informatie die verband houdt met een ernstige wanpraktijk, publiek te maken. De registratie van dergelijke personen als eindgebruiker van elektronische-communicatiediensten heeft bijgevolg een rechtstreekse impact op de informatiestroom in de richting van de pers en in de richting van politici.

Bovendien gaat de onmogelijkheid voor journalisten en politici om op anonieme wijze kennis te nemen van maatschappelijk belangrijke informatie, verder dan strikt noodzakelijk is in het licht van die doelstellingen. Die onmogelijkheid zet immers essentiële democratische controlemechanismen op de helling.

A.25.1. Volgens de Ministerraad hebben de verzoekende partijen geen belang bij dat onderdeel, aangezien zij geen journalisten zijn. Overigens viseert dat onderdeel niet zozeer de bestreden bepalingen, maar veeleer de wet van 29 mei 2016.

A.25.2. Ten gronde is het niet de bedoeling van de bestreden bepalingen om de persvrijheid aan banden te leggen, des te meer daar het bronnengeheim van de journalist slechts zal worden opgeheven om een dreigende inbreuk op de fysieke integriteit van personen tegen te gaan. Indien de fysieke integriteit van personen reeds is aangetast, kan het bronnengeheim niet worden opgeheven. Aangezien de bestreden bepalingen passen in het kader van de opsporing en vervolging van zware misdaden, zullen zij bijgevolg niet worden toegepast om het bronnengeheim te omzeilen. In zoverre zich toch een situatie zou voordoen waarin het bronnengeheim van een journalist moet worden opgeheven vanwege de bescherming van de fysieke integriteit van derden, wordt dit blijkens de rechtspraak van het Hof verantwoord wegens de ernst en het vaak onherstelbare karakter van de misdrijven die een ernstige bedreiging opleveren voor de fysieke integriteit.

A.26.1. De verzoekende partijen zijn van mening dat zij wel belang hebben bij het derde onderdeel van het tweede middel, aangezien de vrijheid van meningsuiting het recht van eenieder om inlichtingen of denkbeelden te ontvangen of te verstrekken, waarborgt. Bovendien zijn de verzoekende partijen allen gemeenteraadsleden in de gemeente Brecht, die in het kader van hun politieke activiteiten anoniem willen kunnen bellen.

Bovendien is het onjuist te beweren dat het middelonderdeel betrekking heeft op de wet van 29 mei 2016. Het is de bestreden wet die de anonimiteit van de vooraf betaalde kaart afschaft en het voor de verzoekende partijen onmogelijk maakt om nog anoniem elektronische-communicatiediensten te gebruiken.

A.26.2. Ten gronde beklemtonen de verzoekende partijen dat de bestreden wet de anonimiteit van de vooraf betaalde kaart afschaft ten aanzien van alle eindgebruikers, zonder in een uitzondering te voorzien voor journalisten. Aldus wordt het journalistieke bronnengeheim in alle gevallen beperkt.

A.27. In hun aanvullende memorie wijzen de verzoekende partijen erop dat het Hof van Justitie bij zijn arrest van 6 oktober 2020 in zake *La Quadrature du Net e.a.* (C-511/18), de doorzending van verkeers- en lokalisatiegegevens als een beperking van de vrijheid van meningsuiting en van communicatie heeft gekwalificeerd, en daaraan heeft toegevoegd dat die vaststelling met name geldt voor de personen wier communicatie onder het beroepsgeheim valt en voor journalisten en klokkenluiders. De veelheid aan bewaarde gegevens kan immers een ontmoedigend effect hebben op de activiteiten van die personen. Diezelfde redenering geldt volgens de verzoekende partijen voor loutere identificatiegegevens.

Ten aanzien van het derde middel

A.28. In hun derde middel voeren de verzoekende partijen aan dat artikel 2 van de bestreden wet niet bestaanbaar is met 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, met de artikelen 48, 49 en 52 van het Handvest van de grondrechten van de Europese Unie, met het algemeen rechtsbeginsel van het recht op een eerlijk proces en van het recht van verdediging, waaronder het vermoeden van onschuld, en met het wettigheidsbeginsel in strafzaken.

Het bij de bestreden bepaling ingevoerde vermoeden van toerekenbaarheid, krachtens hetwelk de geïdentificeerde natuurlijke persoon of rechtspersoon behoudens tegenbewijs verantwoordelijk is voor het gebruik van de elektronische-communicatiedienst die aan hem wordt verstrekt, niet evenredig is met de doelstelling om het doorgeven van vooraf betaalde kaarten aan derden te voorkomen.

A.29.1. Het vermoeden van toerekenbaarheid schendt het wettigheidsbeginsel in strafzaken, aangezien de draagwijdte ervan onduidelijk is. Er kan niet worden uitgemaakt of het gaat om een contractuele aansprakelijkheid ten aanzien van de operator, om een aquiliaanse aansprakelijkheid ten aanzien van derden, of om een strafrechtelijke verantwoordelijkheid. In de memorie van toelichting werd daarop slechts geantwoord dat het vermoeden van toerekenbaarheid het onmogelijk moet maken dat een persoon zich identificeert in plaats van een derde die de elektronische-communicatiedienst daadwerkelijk gebruikt, om op die manier de identiteit van die derde te verbergen. Door haar vage formulering verheldert de bestreden bepaling niet, maar sluit zij evenmin uit dat het vermoeden van toerekenbaarheid de strafrechtelijke verantwoordelijkheid van de geïdentificeerde eindgebruiker kan bepalen.

A.29.2. Een dergelijk vermoeden van toerekenbaarheid staat niet in een redelijk verband van evenredigheid met de nagestreefde doelstelling. De bestreden bepaling verbiedt niet om een vooraf betaalde kaart aan te kopen in opdracht van een derde of om die kaart later aan een derde door te verkopen. Artikel 5 van het koninklijk besluit van 27 november 2016 voorziet in de mogelijkheid om een vooraf betaalde kaart over te dragen aan bepaalde derden. Maar daarnaast kan een telefoontoestel ook worden gestolen, of kunnen derden onder valse voorwendselen eindgebruikers te goeder trouw ertoe aanzetten om hun telefoontoestel aan hen ter beschikking te stellen.

Het toepassingsgebied van het vermoeden van toerekenbaarheid wordt overigens niet beperkt tot terroristische misdrijven of tot zware misdaden. Het vermoeden blijkt van toepassing te zijn op alle misdrijven. Daardoor is het voor de eindgebruikers onmogelijk te weten welke daden of nalatigheden hun strafrechtelijke verantwoordelijkheid in het geding brengen. Nochtans kan een eindgebruiker die te goeder trouw zijn vooraf betaalde kaart ter beschikking stelt van een derde, onmogelijk weten welke feiten die derde van plan is te plegen. Hij mag het gebruik door die derde ook niet controleren, aangezien dat strafbaar is krachtens artikel 124 van de wet van 13 juni 2005 en artikel 314*bis* van het Strafwetboek.

A.29.3. Het vermoeden van toerekenbaarheid impliceert ook dat de eindgebruiker die zijn vooraf betaalde kaart laat gebruiken door de dader van een terroristisch misdrijf, zelf kan worden vervolgd op basis van de artikelen 140 en 141 van het Strafwetboek. Hij zal immers, indien hij er niet in slaagt het tegenbewijs te leveren, strafrechtelijk worden veroordeeld wegens het ter beschikking stellen van communicatiemiddelen voor het plegen van terroristische misdrijven.

A.29.4. Het tegenbewijs waarin de bestreden wet voorziet, valt redelijkerwijs niet te leveren, aangezien de geïdentificeerde eindgebruiker onmogelijk op de hoogte kan zijn van het gebruik dat de derde maakt van de elektronische-communicatiedienst.

A.30.1. Volgens de Ministerraad kan een weerlegbaar vermoeden onmogelijk het vermoeden van onschuld schenden. De bestreden bepaling voegt overigens weinig toe aan het uitgangspunt dat in elk gerechtelijk onderzoek geldt, namelijk dat de gebruiker van een telefoonlijn aan de basis van de communicatie ligt. Dit is evenzeer het geval bij het gebruik van vaste lijnen of bij het gebruik van abonnementen. De bestreden bepaling doet evenmin afbreuk aan het vermoeden van onschuld, aangezien zij niet wegneemt dat de betrokkene wordt vermoed onschuldig te zijn tot bewijs van het tegendeel. Indien de gebruiker aannemelijk kan maken dat hij zijn communicatiemiddel niet heeft gebruikt op het ogenblik van de feiten, kan hij niet worden veroordeeld. Het is vaste cassatierechtspraak dat de verdachte vrijuit moet gaan indien zijn uitleg materieel mogelijk is en niet wordt tegengesproken door de stukken van het dossier.

Het Grondwettelijk Hof oordeelt dat wettelijke vermoedens in beginsel niet strijdig zijn met het vermoeden van onschuld, voor zover zij in een redelijk verband van evenredigheid staan met een legitieme doelstelling, waarbij rekening dient te worden gehouden met de ernst van de zaak en waarbij de rechten van verdediging moeten worden gevrijwaard.

A.30.2. Volgens de Ministerraad legt de bestreden bepaling zelf geen strafsanctie op. Het doorgeven van een vooraf betaalde kaart aan derden wordt dus niet strafrechtelijk gesanctioneerd. Bijgevolg is de verwijzing van de verzoekende partijen naar het strafrechtelijk wettigheidsbeginsel en naar het beginsel van de evenredigheid van de straf naast de kwestie.

A.31. De verzoekende partijen zijn van mening dat het aan het Hof staat te beoordelen hoe de bestreden bepaling dient te worden geïnterpreteerd, en niet aan de Ministerraad. In elk geval blijkt dat de draagwijdte van de bestreden bepaling onduidelijk is en dus op gespannen voet staat met het strafrechtelijk wettigheidsbeginsel. Het lijkt erop dat de bestreden bepaling niet alleen een vermoeden van gebruik, maar een vermoeden van schuld, en dus een omkering van bewijslast invoert. Dat vermoeden wijkt af van het beginsel dat de bewijslast in strafzaken op de vervolgende partij rust.

A.32. Volgens de verzoekende partijen verandert het arrest van het Hof nr. 57/2021 van 22 april 2021 niets aan de bevoegdheid van de procureur des Konings of de onderzoeksrechter om de abonnee of gewoonlijke gebruiker van een elektronische communicatiedienst te identificeren. Het bestreden vermoeden van toerekenbaarheid blijft bijgevolg relevant.

Ten aanzien van het vierde middel

A.33. In hun vierde middel voeren de verzoekende partijen aan dat artikel 3 van de bestreden wet niet bestaanbaar is met 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, 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. Het middel valt uiteen in vijf onderdelen.

A.34.1. In het eerste onderdeel van het vierde middel klagen de verzoekende partijen aan dat de toegang tot de op grond van de bestreden wet verzamelde en bewaarde identificatiegegevens door de inlichtingen- en veiligheidsdiensten, een ongerechtvaardigde beperking van de bescherming van de persoonlijke levenssfeer vormt.

A.34.2. De bestreden bepaling laat de inlichtingen- en veiligheidsdiensten toe de medewerking van een bank of financiële instelling te vorderen om over te gaan tot het identificeren van de eindgebruiker van een vooraf betaalde kaart. Het betreft dus een toegang tot persoonsgegevens die zijn verwerkt op grond van de wet van 29 mei 2016. Een dergelijke procedure vormt een inmenging in het recht op eerbiediging van het privé- en gezinsleven.

Uit de rechtspraak van het Hof van Justitie blijkt dat een dergelijke beperking moet berusten op één van de doelstellingen die limitatief zijn vermeld in artikel 15, lid 1, eerste zin, van de richtlijn 2002/58/EG. Doelstellingen die te maken hebben met de bestrijding van misdrijven, mogen, gelet op de aard van de in het geding zijnde beginselen, slechts betrekking hebben op zware misdaden. Bovendien mag de toegang tot de verwerkte persoonsgegevens niet verder gaan dan strikt noodzakelijk is om die doelstelling te bereiken. Tot slot moet het wetgevend kader de materiële en procedurele voorwaarden van de toegang bepalen, alsook adequate waarborgen bevatten om misbruik van die gegevens tegen te gaan. De naleving van die voorwaarden moet het voorwerp uitmaken van een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit.

A.34.3. Het bij de bestreden bepaling gewijzigde artikel 16/2, §§ 2 tot 4, van de wet van 30 november 1998 « houdende regeling van de inlichtingen- en veiligheidsdiensten » biedt volgens de verzoekende partijen onvoldoende waarborgen. Het onderwerpt de identificatie van de eindgebruiker van vooraf betaalde kaarten aan de gewone methode voor het verzamelen van gegevens. Dit impliceert dat die gegevens mogen worden gebruikt door de inlichtingen- en veiligheidsdiensten telkens wanneer dat in het belang van de uitoefening van hun opdrachten is. Aldus kunnen zij toegang tot de verzamelde gegevens vragen, en daarvoor desnoods de medewerking van een bank of een financiële instelling vorderen, los van een potentiële terroristische dreiging en los van de bestrijding van de zware misdaad.

Daarnaast beperkt de bestreden bepaling de toegang tot de identificatiegegevens van de eindgebruiker niet tot verdachten van zware misdaden of van terroristische activiteiten. Evenmin somt zij de objectieve elementen op die een toegang tot die gegevens kunnen verantwoorden. Aldus gaat zij verder dan strikt noodzakelijk is in het licht van de nationale veiligheid, de staatsveiligheid, de openbare veiligheid en de bestrijding van zware misdaden.

A.35.1. In het tweede onderdeel van het vierde middel klagen de verzoekende partijen aan dat de toegang tot de op grond van de bestreden wet verzamelde en bewaarde identificatiegegevens door de inlichtingen- en veiligheidsdiensten niet bestaanbaar is met het recht op bescherming van de persoonlijke levenssfeer, doordat de toegang tot de bewaarde gegevens niet afhankelijk wordt gemaakt van een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke autoriteit.

A.35.2. Het bij de bestreden bepaling gewijzigde artikel 16/2, § 2, van de wet van 30 november 1998 onderwerpt de vordering door de inlichtingen- en veiligheidsdiensten van de medewerking van een bank of een financiële instelling om de eindgebruiker van een vooraf betaalde kaart te identificeren, niet aan een rechterlijke controle. De vordering geschiedt immers door het diensthoofd of zijn afgevaardigde. In beginsel gaat het om de administrateur-generaal van de Veiligheid van de Staat. De vordering is niet onderworpen aan een voorafgaand eensluidend advies van de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, bedoeld in artikel 43/1 van de wet van 30 november 1998. Evenmin wordt voorzien in enige voorafgaande rechterlijke controle.

A.36.1. In het derde onderdeel van het vierde middel klagen de verzoekende partijen aan dat de toegang tot de op grond van de bestreden wet verzamelde en bewaarde identificatiegegevens door de inlichtingen- en veiligheidsdiensten niet bestaanbaar is met het recht op bescherming van de persoonlijke levenssfeer, doordat de bestreden bepaling geen materiële en procedurele voorwaarden voor de toegang tot de bewaarde gegevens bevat.

A.36.2. De bestreden bepaling vermeldt alleen dat de toegang tot de bewaarde identificatiegegevens geschiedt « op vordering », en dat die vordering schriftelijk dient te worden ingediend, behoudens hoogdringendheid. De vordering moet niet met redenen zijn omkleed. Ook de aard van de opgevraagde gegevens wordt niet nader toegelicht. Evenmin worden de materiële en de procedurele voorwaarden waaraan de vordering dient te voldoen, nader gepreciseerd. Nochtans worden de banken en de financiële instellingen onder druk gezet om op die vordering in te gaan, aangezien zij anders krachtens artikel 16/2, § 3, van de wet van 30 november 1998 een geldboete van zesentwintig euro tot tienduizend euro, vermeerderd met opdeciemen, riskeren.

A.37. In het vierde onderdeel van het vierde middel klagen de verzoekende partijen aan dat de toegang tot de op grond van de bestreden wet verzamelde en bewaarde identificatiegegevens door de inlichtingen- en veiligheidsdiensten niet bestaanbaar is met het recht op bescherming van de persoonlijke levenssfeer, doordat de bestreden bepaling niet regelt dat de inlichtingen- en veiligheidsdiensten die toegang hebben gehad tot de verwerkte persoonsgegevens, de betrokken eindgebruiker daarvan op de hoogte moeten brengen, en doordat zij niet voorziet in een daadwerkelijke rechterlijke controle, zowel in feite als in rechte, op de rechtmatigheid van die toegang.

A.38. In het vijfde onderdeel van het vierde middel klagen de verzoekende partijen aan dat de toegang tot de op grond van de bestreden wet verzamelde en bewaarde identificatiegegevens door de inlichtingen- en veiligheidsdiensten niet bestaanbaar is met het recht op bescherming van de persoonlijke levenssfeer, doordat de bestreden bepaling niet uitsluit dat buitenlandse inlichtingen- en veiligheidsdiensten toegang krijgen tot de bewaarde identificatiegegevens. Artikel 20 van de wet van 30 november 1998 maakt een dergelijke uitwisseling van persoonsgegevens zelfs uitdrukkelijk mogelijk. Die bepaling maakt geen enkel onderscheid naar gelang van de aard van de meegedeelde gegevens of het nut ervan voor lopende onderzoeken.

A.39.1. De Ministerraad is van mening dat de vijf onderdelen van het vierde middel in wezen tot één rechtsvraag terug te brengen zijn. Dat middel is overigens niet ontvankelijk in zoverre het Hof wordt verzocht om de bestreden bepaling te toetsen aan de richtlijnen 95/46/EG en 2002/58/EG.

In elk geval blijkt dat de toegang van de veiligheids- en inlichtingendiensten tot bepaalde bankgegevens, met name de gegevens die de identificatie van de eindgebruiker van een vooraf betaalde kaart mogelijk maken, geen betrekking hebben op persoonsgegevens, zodat de richtlijn 2002/58/EG niet van toepassing is. Artikel 1, lid 1, van de richtlijn 2002/58/EG en artikel 3, lid 1, van de richtlijn 95/46/EG bepalen immers dat die richtlijnen niet van toepassing zijn op de verwerking van persoonsgegevens die voortkomen uit activiteiten van de veiligheid van de Staat, de landsverdediging, de openbare veiligheid, en het voorkomen, het onderzoeken, het opsporen en vervolgen van strafbare feiten of schendingen van de beroepscode voor gereglementeerde beroepen.

De bestreden bepaling maakt deel uit van het straf- en strafprocesrecht, de openbare veiligheid en de bescherming en de veiligheid van de Staat. Die materies vallen niet onder het toepassingsgebied van het Europees Unierecht.

A.39.2. De verwijzing van de verzoekende partijen naar de rechtspraak van het Hof van Justitie is volgens de Ministerraad naast de kwestie. Het arrest van het Hof van Justitie van 21 december 2016 in zake *Tele2 Sverige* (C-203/15 en C-698/15) handelde immers over verkeers- en lokalisatiegegevens, terwijl artikel 16/2 van de wet van 30 november 1998 slechts betrekking heeft op identificatiegegevens.

Zelfs indien de lering uit dat arrest zou moeten worden doorgetrokken, dient te worden vastgesteld dat de mogelijke inmenging in het privé- en gezinsleven veel beperkter is wanneer loutere identificatiegegevens in het geding zijn. Die gegevens laten op zich immers niet toe de bron, de bestemmeling, de datum, het tijdstip, de duur en de aard van een communicatie te bepalen. Ook de frequentie van de communicaties tussen twee personen kan niet op basis van die gegevens worden vastgesteld. De loutere identificatiegegevens laten bijgevolg niet toe precieze conclusies te trekken over het privéleven van personen van wie die gegevens worden bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties of de kringen waarin zij verkeren.

De vraag rijst dus of er wel sprake is van een inmenging in het privé- en gezinsleven indien enkel de medewerking van een bank of een financiële instelling wordt gevorderd om over te gaan tot het identificeren van de eindgebruiker van een vooraf betaalde kaart.

A.39.3. Tot slot bevat de wet van 30 november 1998 voldoende waarborgen ter bescherming van de persoonlijke levenssfeer. Daarom dient de vordering te worden ondertekend door het diensthoofd of zijn

gedelegeerde. Bovendien moet de dienst voor de Veiligheid van de Staat een lijst bijhouden van alle gevorderde identificaties en moet hij iedere maand een lijst van de gevorderde gegevens doorsturen aan het Comité I. Die waarborgen volstaan in het licht van de zeer beperkte inmenging in het privé- en gezinsleven die uit de bestreden bepaling kan voortvloeien.

A.40.1. Volgens de verzoekende partijen is de richtlijn 2002/58/EG van toepassing, aangezien deze betrekking heeft op alle verwerkingen van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare communicatienetwerken, alsook op elke persoon die hierdoor indirect of direct kan worden geïdentificeerd. Die richtlijn maakt geen enkel onderscheid naar gelang van de materie.

Aangezien de operatoren worden verplicht om de referentie van de banktransacties waarmee de vooraf betaalde kaart wordt aangekocht, op te slaan, en de inlichtingen- en veiligheidsdiensten zich toegang kunnen verschaffen tot die gegevens, gaat het om een verwerking van persoonsgegevens in het kader van elektronische-communicatiediensten, zodat de richtlijn 2002/58/EG van toepassing is.

A.40.2. Het door de Ministerraad gemaakte onderscheid tussen verkeers- en lokalisatiegegevens, enerzijds, en loutere identificatiegegevens, anderzijds, doet volgens de verzoekende partijen niet ter zake. Van belang is enkel dat persoonsgegevens worden verwerkt met het oog op de staatsveiligheid, en dat de nationale autoriteiten daar toegang toe hebben. In die zin is de verwijzing naar het voormelde arrest van het Hof van Justitie van 21 december 2016 wel degelijk relevant.

Bovendien kunnen de bewaarde identificatiegegevens niet worden losgekoppeld van de bewaarde lokalisatie- en communicatiegegevens. Zodra een overheid krachtens de bestreden wet een eindgebruiker van een elektronische-communicatiedienst heeft geïdentificeerd, kan zij die gegevens immers zelf verbinden met de andere persoonsgegevens die over de betrokkene werden verwerkt, waaronder zijn lokalisatie- en communicatiegegevens. Aldus is een identificatie van de eindgebruiker een eerste stap in de verregaande inmenging in het privé- en gezinsleven zoals die door de Ministerraad werd beschreven.

A.40.3. De drie door de Ministerraad opgesomde waarborgen volstaan geenszins in het licht van een dergelijke beperking van het recht op eerbiediging van het privé- en gezinsleven, zoals ook blijkt uit de voormelde rechtspraak van het Hof van Justitie van de Europese Unie. Om in overeenstemming te zijn met die rechtspraak, had de bestreden wet moeten bepalen dat de toegang tot de bewaarde gegevens slechts kan worden verleend in het kader van de bestrijding van zware misdaden, had zij die toegang aan het voorafgaande oordeel van een rechterlijke instantie of van een onafhankelijke bestuurlijke commissie moeten onderwerpen, had zij de materiële en procedurele voorwaarden van die toegang moeten regelen, had zij moeten bepalen dat de geïdentificeerde eindgebruikers op de hoogte moeten worden gebracht van elke toegang tot hun identificatiegegevens en hun in dat kader een daadwerkelijke toegang tot de rechter moeten toekennen, en had zij moeten bepalen dat de identificatiegegevens niet mogen worden uitgewisseld met buitenlandse inlichtingen- en veiligheidsdiensten.

A.41. De Ministerraad benadrukt dat de bestreden bepaling geen betrekking heeft op identificatiegegevens, maar op de toegang tot bankgegevens. Hierop zijn de in het middel vermelde toetsingsnormen, en minstens de in het middel vermelde richtlijnen 95/46/EG en 2002/58/EG, niet van toepassing.

Het feit dat de eindgebruiker niet in kennis wordt gesteld van de verwerking van en toegang tot zijn persoonsgegevens, wordt verklaard door de eigenheid van het werk van de inlichtingen- en veiligheidsdiensten, dat erin bestaat de veiligheid van de Staat te waarborgen, onder meer tegen terroristische aanslagen. Die diensten hebben geen gerechtelijke finaliteit en de verwerkte persoonsgegevens worden niet gebruikt in strafzaken.

A.42. In hun aanvullende memorie wijzen de verzoekende partijen erop dat het arrest nr. 57/2021 van 22 april 2021 de regels inzake de toegang van de inlichtingen- en veiligheidsdiensten tot de bewaarde identificatiegegevens niet heeft gewijzigd. Ook het arrest van het Hof van Justitie van 6 oktober 2020 in zake *La Quadrature du Net e.a.* (C-511/18) heeft geen invloed op het vierde middel.

Wel dient volgens hen te worden verwezen naar het arrest van het Hof van Justitie van 2 maart 2021 in zake *Prokuratuur* (C-746/18), waarin het Hof van Justitie heeft gedefinieerd wat dient te worden verstaan onder de « onafhankelijke bestuurlijke autoriteit » die moet instaan voor het voorafgaande toezicht op de toegang van de inlichtingen- en veiligheidsdiensten tot de verwerkte persoonsgegevens. Die instantie moet bevoegd zijn om alle betrokken belangen en rechten met elkaar in overeenstemming te brengen en zij moet haar taken objectief en onpartijdig kunnen uitoefenen zonder enige invloed van buitenaf.

Aangezien artikel 16/2, § 2, van de wet van 30 november 1998 slechts een toelating van het diensthoofd of zijn afgevaardigde vereist, zonder voorafgaande machtiging van de BIM-commissie, is *in casu* geen sprake van een onafhankelijke bestuurlijke autoriteit. Bovendien waarborgt de bestreden bepaling niet dat de toegang van de inlichtingen- en veiligheidsdiensten tot de verwerkte persoonsgegevens beperkt blijft tot gevallen waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid op het spel staan.

Zij waarborgt evenmin dat de betrokkene kennis krijgt van die toegang opdat hij zijn recht op jurisdictionele controle zou kunnen uitoefenen. Nochtans heeft het Hof bij zijn arrest nr. 41/2019 van 14 maart 2019 de wetgever verplicht om te voorzien in een mechanisme van actieve kennisgeving waarmee de betrokkene ervan in kennis wordt gesteld dat hij het voorwerp heeft uitgemaakt van een maatregel van geheim toezicht door de veiligheids- en inlichtingendiensten.

Tot slot wijzen de verzoekende partijen erop dat bij wet van 30 maart 2017 de maandelijkse toezending aan het Comité I van de lijst van gevorderde gegevens is afgeschaft. Die waarborg waarnaar de Ministerraad verwijst, is bijgevolg weggevallen.

Ten aanzien van de handhaving

A.43. In hun aanvullende memorie wijzen de verzoekende partijen tot slot erop dat het Hof van Justitie bij zijn arrest van 6 oktober 2020 in zake *La Quadrature du Net e.a.* (C-511/18) heeft geoordeeld dat het Grondwettelijk Hof de wetsbepalingen die in strijd met dat arrest waren, diende te vernietigen, zonder de gevolgen ervan te mogen handhaven. Bijgevolg kunnen ook de gevolgen van de bestreden wet niet worden gehandhaafd.

- B -

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 identificatieverplichting 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 evenredigheidsbeginsel 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 elektronischecommunicatiedienst 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 interconnectiebetalingen 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 communicatienetwerken (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 persoonsgegevens 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 internettelefonieaccount;

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