Voor eensluidend verklaard afschrift. Mr. Raf Jespers

BEROEP TOT NIETIGVERKLARING

Aan de Dames en Heren Voorzitters en Rechters die het Grondwettelijk Hof van België samenstellen,

Mevrouwen,
Mijn Heren,

Geeft U met de meeste eerbied te kennen :

1. **V.Z.W. LIGA VOOR MENSENRECHTEN** ingeschreven in de kruispuntbank voor ondernemingen onder het ondernemingsnummer 0419.191.537, met zetel te 9000 GENT, Gebroeders De Smetstraat 75;

- eerste verzoekster -

2. **A.S.B.L LIGUE DES DROITS DE L'HOMME,** ingeschreven in de kruispuntbank voor ondernemingen onder het ondernemingsnummer 0410.105.805, met zetel te 1000 BRUSSEL, Kogelstraat 22;

- tweede verzoekster –

Verder genoemd verzoekers,

Beiden met als raadsman, Mter. Raf JESPERS, advocaat te 2018 ANTWERPEN, Broederminstraat 38;

Bij wie verzoekers keuze van woonplaats doen voor deze procedure.

Dat zij bij huidig verzoekschrift overeenkomstig de artikelen 1, 2, 5 en 6 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof wegens schending van de regels die door of krachtens de Grondwet zijn vastgesteld voor het bepalen van de onderscheiden bevoegdheid van de Staat, de Gemeenschappen en de Gewesten of van de artikelen van titel II « De Belgen en hun rechten », en de artikelen 170, 172 en 191 van de Grondwet een beroep instelt tot de gehele of gedeeltelijke vernietiging van:

De artikels 1 tot en met 7 van de wet van 30 juli 2013 tot wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies

van het Wetboek van strafvordering (bekendgemaakt in het Belgisch Staatsblad van 23 augustus 2013);

Verzoekers voegen overeenkomstig artikel 7, eerste lid van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof bij dit verzoekschrift een afschrift van de bestreden wet en, in voorkomend geval, van de bijlagen ervan (stuk 1).

Inhoudstafel

I. Het voorwerp van de procedure - de bestreden wet, decreet of in artikel 134 van de Grondwet bedoelde regel

1.

Verzoekers stellen een beroep tot vernietiging in van de artikels 1 tot en met 7 van de wet van 30 juli 2013 tot wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van strafvordering (bekendgemaakt in het Belgisch Staatsblad van 23 augustus 2013 (hierna: de bestreden wet).

2.

Het dispositief van de bestreden wet luidt als volgt (stuk 1):

HOOFDSTUK 1. - Doel

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

Art. 2. Deze wet zet 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 en tot wijziging van Richtlijn 2002/58/EG ("Dataretentierichtlijn") (Publicatieblad, 13 april 2006, L 105/54) en artikel 15.1 van 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") (Publicatieblad, 31 juli 2002, L 201/37) gedeeltelijk om in Belgisch recht.

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

Art. 3. Artikel 1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, gewijzigd bij de wet van 10 juli 2012, wordt aangevuld met een lid luidende :

" Deze wet voorziet in een gedeeltelijke omzetting 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 en tot wijziging van Richtlijn 2002/58/EG ("Dataretentierichtlijn") (Publicatieblad 13 april 2006, L 105/54) en van artikel 15.1 van 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") (Publicatieblad, 31 juli 2002, L 201/37). ".

Art. 4. In artikel 2 van dezelfde wet, gewijzigd bij de wetten van 18 mei 2009 en 10 juli 2012, worden de volgende wijzigingen aangebracht:

a) het 11° wordt vervangen door wat volgt :
" 11° "operator" : een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9; ";

b) het artikel wordt aangevuld met een 74° luidende als volgt :
" 74° "Oproeppoging zonder resultaat" : een communicatie waarbij een oproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord. ".

Art. 5. Artikel 126 van dezelfde wet wordt vervangen als volgt:

"Art. 126. § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bewaren de aanbieders van aan het publiek aangeboden vaste telefoniediensten, mobiele telefoniediensten, internettoegangdiensten, internet-e-maildiensten, of internettelefoniediensten, en de aanbieders van de onderliggende openbare elektronische-communicatienetwerken de verkeersgegevens, de locatiegegevens, de gegevens voor identificatie van de eindgebruikers, de gegevens voor identificatie van de gebruikte elektronische-communicatiedienst en de gegevens voor identificatie van de vermoedelijk gebruikte eindapparatuur, die door hen worden gegenereerd of verwerkt bij het leveren van de betreffende communicatiediensten.
Onder aanbieders in de betekenis van dit artikel worden ook de doorverkopers in eigen naam en voor eigen rekening verstaan.
Onder telefoniedienst in de betekenis van dit artikel wordt verstaan : telefoonoproepen - met inbegrip van spraakoproepen, voicemail, conference call of datacommunicatie-, aanvullende diensten - met inbegrip van call forwarding en call transfer -, en de messaging- en multimediadiensten - met inbegrip van short message service (sms), enhanced media service (EMS) en multimedia service (MMS).
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 krachtens het eerste lid te bewaren gegevens per type dienst alsook de vereisten waaraan deze gegevens moeten beantwoorden.
Behoudens andersluidende wettelijke bepaling, mogen geen gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, bewaard worden.
De verplichting om de in het eerste lid bedoelde gegevens te bewaren, is ook van toepassing op oproeppogingen zonder resultaat, voor zover die gegevens in verband met de aanbieding van de bedoelde communicatiediensten:

1° wat de telefoniegegevens betreft, worden gegenereerd, verwerkt en opgeslagen door de aanbieders van openbare diensten voor elektronische communicatie of van een openbaar netwerk voor elektronische communicatie, of

2° wat de internetgegevens betreft, door deze aanbieders worden gelogd.

§ 2. De gegevens bedoeld in paragraaf 1, eerste lid, worden bewaard met het oog op :

de opsporing, het onderzoek en de vervolging van strafbare feiten zoals bedoeld in de artikelen 46bis en 88bis van het Wetboek van strafvordering;

de beteugeling van kwaadwillige oproepen naar de nooddiensten, zoals bedoeld in artikel 107;

het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of -dienst, zoals bedoeld in artikel 43bis, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

de vervulling van de inlichtingenopdrachten met inzet van de methoden voor het verzamelen van gegevens zoals bedoeld in de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de gegevens opgenomen in paragraaf 1, eerste lid, onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en op eenvoudig verzoek aan de autoriteiten belast met de opdrachten bedoeld in de punten a) tot d) kunnen worden meegedeeld en uitsluitend aan deze laatsten.

§ 3. De gegevens ter identificatie van de eindgebruikers, de gebruikte elektronische-communicatiedienst en de vermoedelijk gebruikte eindapparatuur worden bewaard vanaf de inschrijving op de dienst, zolang binnenkomende of uitgaande communicatie mogelijk is door middel van de dienst waarop werd ingetekend en gedurende twaalf maanden vanaf de datum van de laatste geregistreerde binnenkomende of uitgaande communicatie.

De verkeers- en localisatiegegevens worden bewaard gedurende twaalf maanden 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 gegevens die zijn onderworpen aan het eerste lid en deze die zijn onderworpen aan het tweede lid.

§ 4. Naar aanleiding van het evaluatieverslag bedoeld in paragraaf 7, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer, de bewaringstermijn van de gegevens voor bepaalde categorieën van gegevens aanpassen, zonder een termijn van meer dan 18 maanden vast te leggen.

De Koning kan, in de omstandigheden zoals bedoeld in artikel 4, § 1, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Commissie voor de bescherming van de persoonlijke levenssfeer, voor een beperkte

periode, een bewaringstermijn voor de gegevens vastleggen die langer is dan twaalf maanden.

Wanneer in de omstandigheden bedoeld in het tweede lid de Koning een bewaringstermijn oplegt die langer is dan vierentwintig maanden, stelt de minister de Europese Commissie en de overige lidstaten van de Europese Unie onverwijld in kennis van alle genomen maatregelen, met vermelding van de redenen die eraan ten grondslag liggen.

§ 5. Voor de bewaring van de in paragraaf 1, eerste lid, bedoelde gegevens geldt het onderstaande voor de aanbieder van een netwerk of dienst voor elektronische communicatie bedoeld in paragraaf 1, eerste lid :

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

2° hij zorgt ervoor 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° hij garandeert dat de toegang tot de bewaarde gegevens enkel gebeurt door een of meer leden van de Coördinatiecel Justitie bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie en door het personeel en de aangestelden van deze aanbieders die specifiek door deze cel gemachtigd zijn;

4° hij zorgt ervoor dat de gegevens na afloop van de bewaringstermijn die voor die gegevens geldt, worden vernietigd.

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 technische en administratieve maatregelen die de aanbieders van diensten en netwerken beoogd in paragraaf 1, eerste lid, moeten nemen teneinde de bescherming van de bewaarde persoonsgegevens te garanderen.

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, worden beschouwd als verantwoordelijk voor de verwerking van deze gegevens in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

§ 6. De minister en de Minister van Justitie zorgen ervoor dat jaarlijks aan de Europese Commissie en de Kamer van volksvertegenwoordigers statistische informatie wordt verstrekt over de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare communicatiediensten of -netwerken. Die informatie heeft onder meer betrekking op:

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 niet konden worden ingewilligd.

Deze statistische informatie mag geen persoonsgegevens omvatten.
De gegevens die betrekking hebben op de toepassing van paragraaf 2, a), worden tevens bijgevoegd bij het verslag dat de Minister van Justitie overeenkomstig artikel 90decies 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 van diensten of netwerken jaarlijks moeten overzenden aan het Instituut en deze die het Instituut overzendt aan de minister en aan de Minister van Justitie.

§ 7. Onverminderd het verslag bedoeld in paragraaf 6, derde lid, brengen de minister en de Minister van Justitie, twee jaar na de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 1, derde lid, aan de Kamer van volksvertegenwoordigers een evaluatieverslag uit 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. ".

Art. 6. In artikel 145 van dezelfde wet, gewijzigd bij de wet van 25 april 2007, wordt een paragraaf 3ter ingevoegd, luidende :

" § 3ter. Met geldboete van 50 euro tot 50.000 euro en met gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft :
1° iedere persoon die, naar aanleiding van de uitoefening van zijn functie, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de gegevens bedoeld in artikel 126 op enige manier overneemt, onder zich houdt, of er enig gebruik van maakt;
2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt. ".

HOOFDSTUK 3. - Wijziging van artikel 90decies van het Wetboek van strafvordering

Art. 7. Artikel 90decies van het Wetboek van strafvordering, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 8 april 2002, 7 juli 2002 en 6 januari 2003, wordt aangevuld met een lid, luidende :

" Bij dit verslag wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, § 6, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie. "

II. Ontvankelijkheid van het beroep

A. Met betrekking tot het belang

3.

Wanneer een vereniging zonder winstoogmerk die niet haar persoonlijk belang aanvoert, voor het Hof optreedt, is vereist dat haar maatschappelijk doel van bijzondere aard is en, derhalve, onderscheiden van het algemeen belang; dat zij een collectief belang verdedigt; dat haar maatschappelijk doel door de bestreden norm kan worden geraakt; dat ten slotte niet blijkt dat dit maatschappelijk doel niet of niet meer werkelijk wordt nagestreefd.[1]

1. Ten aanzien van eerste verzoekster VZW LIGA VOOR MENSENRECHTEN

4.

Eerste verzoekster, V.Z.W. LIGA VOOR MENSENRECHTEN, is een vereniging zonder winstoogmerk naar Belgisch recht en heeft rechtspersoonlijkheid.

Artikel 3 van haar statuten bepaalt (stuk 2):

> *"De vereniging heeft tot doel elke onrechtvaardigheid en elke aanslag op de rechten van personen of gemeenschappen te bestrijden.*
> *Zij verdedigt de beginselen van gelijkheid, vrijheid en humanisme, waarop de democratische maatschappijen gebaseerd zijn, en die onder meer vervat zijn in de Verklaring van de Rechten van de Mens van 1789, bekrachtigd door de Belgische Grondwet van 1831, de Universele Verklaring van de Rechten van de Mens van 1948, de verdragen met betrekking tot de burgerlijke en politieke rechten, evenals de economische, sociale en culturele rechten, en het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden van 1950.*
> *De vereniging streeft haar doeleinden na los van elke politieke of confessionele binding.*
> *De Liga voor Mensenrechten is een dienst die begeleiding en ondersteuning verleent aan sociaal-culturele organisaties, en meer in het bijzonder rond thema's als gevangeniswezen, racisme, asielrecht, privacy, kinderrechten en mensenrechten in het algemeen."*

Artikel 4 van de statuten bepaalt:

> "*De vereniging kan alle daden stellen en acties ondernemen nodig voor het verwezenlijken van haar doel, zoals onder meer het uitgeven van publicaties, het houden*

[1] Zie onder andere GwH 11 maart 2009, nr. 40/2009; GwH 10 juli 2008, nr. 101/2008; GwH 13 juli 2005, nr. 124/2005; GwH 23 maart 2005, nr. 62/2005; GwH 17 december 2003, nr. 166/2003; GwH 8 mei 2002, nr. 77/2002.

van vergaderingen, het tussenkomen bij de overheden, het indienen van klachten bij de gerechtelijke overheden en het instellen van rechtsgedingen. "

Het maatschappelijk doel van de eerste verzoekster is bijgevolg van bijzondere aard en onderscheiden van het algemeen belang.

5.
De bestreden wet komt tegemoet aan de verplichte omzetting van de Europese Richtlijn 2006/24/EG en regelt de verplichting voor aanbieders van telecom- en internetdiensten om specifieke persoonsgegevens te bewaren teneinde de beschikbaarheid voor overheidsdiensten te garanderen.

Dergelijke regeling is van aard om de grondrechten aan te tasten, in het bijzonder het recht op de eerbiediging van de persoonlijke levenssfeer en bescherming van persoonlijke data, het recht op vertrouwelijkheid van communicatie, het recht op persoonlijke vrijheid en vrijheid van meningsuiting, vergadering en vereniging, de persvrijheid, het recht op eigendom, het beginsel van recht op eerlijk proces en geen straf zonder wet in strafzaken, het recht op een daadwerkelijk rechtsmiddel, alsook het wettigheidsbeginsel in strafzaken, het proportionaliteitsbeginsel, het rechtszekerheidsbeginsel en het evenredigheidsbeginsel en het beginsel van het vermoeden van onschuld.

Deze rechten zijn gewaarborgd door:
-artikelen 5, 6, 7, 8, 10, 11 en 13 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (hierna: EVRM);
-artikel 1 van het 1e aanvullende protocol bij het EVRM, artikel 2 van het 4de aanvullende protocol bij het EVRM;
-artikelen 7, 8, 13 en 52 (1) van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest);
-artikelen 9, 12, 14, 15, 17 en 19 van het Internationaal Verdrag inzake Burgerrechten en Politieke rechten goedgekeurd bij wet van 15 mei 1981 (hierna: IVBPR);
-artikelen 12, 13,14,19, 22, 25, 26 en 27 van de Gecoördineerde Grondwet (hierna: G.W.);
-artikel 544 Burgerlijk Wetboek

Verzoekster steunt haar beroep tot vernietiging op de schending van voormelde en andere vermelde grondrechten.

Het maatschappelijk doel van verzoekster omvat zowel de bescherming van het recht op de eerbiediging van de persoonlijke levenssfeer en bescherming van persoonlijke data, het recht op een eerlijk proces, het recht op persoonlijke vrijheid, het proportionaliteitsbeginsel en het wettigheidsbeginsel in strafzaken. Het maatschappelijk doel van verzoekster kan door de bestreden beslissing (en door het tussen te komen arrest) worden geraakt en verzoekster heeft derhalve belang bij haar tussenkomst.

6.

Uw Grondwettelijk Hof heeft aanvaard dat verzoekster het vereiste belang heeft om een beroep tot nietigverklaring of een vordering tot schorsing in te stellen, dan wel in een zaak tussen te komen in onder andere de volgende arresten:

- GwH 18 juli 2013, nr. 107/2013;
- GwH 14 maart 2013, nr. 37/2013;
- GwH 14 februari 2013, nr.7/2013;
- GwH 6 december 2012, nr. 145/2012;
- GwH 22 september 2011, nr. 145/2011;
- GwH 24 maart 2011, nr. 42/2011;
- GwH 11 maart 2009, nr. 40/2009;
- GwH 10 juli 2008, nr. 101/2008;
- GwH 19 juli 2007, nr. 105/2007;
- GwH 13 juli 2005, nr. 125/2005;
- GwH 23 maart 2005, nr. 62/2005;
- GwH 21 december 2004, nr. 202/2004;
- GwH 17 december 2003, nr. 166/2003;
- GwH 13 november 2002, nr. 167/2002;
- GwH 8 mei 2002, nr. 77/2002;
- GwH 1 maart 2001; nr. 21/2001;
- GwH 25 oktober 2000, nr.106/2000.

7.

Verzoekster legt een uittreksel neer uit de notulen van de vergadering van 7 oktober 2013 waarin haar Raad van Bestuur beslist om het beroep tot vernietiging in te stellen (stuk 3). De Raad van Bestuur is overeenkomstig artikel 13 van de Wet betreffende de verenigingen zonder winstoogmerk, de internationale verenigingen zonder winstoogmerk en de stichtingen bevoegd om deze beslissing te nemen.

Verzoekster legt een uittreksel neer uit de notulen van de vergadering van 3 februari 2014 waarin haar Raad van Bestuur beslist om advocaat Raf Jespers te mandateren voor de procedure (stuk 4).

Het beroep tot vernietiging is bijgevolg ontvankelijk.

<u>Ten aanzien van tweede verzoekster ASBL LIGUE DES DROITS DE L'HOMME</u>

8.

Tweede verzoekster is een vereniging zonder winstoogmerk naar Belgisch recht en heeft rechtspersoonlijkheid.

9.

Tweede verzoekster steunt haar beroep tot vernietiging evenzeer op de schending van de hoger vermelde grondrechten

Volgens haar statuten heeft tweede verzoekster, de ASBL LIGUE DES DROITS DE L'HOMME (stuk 5), tot doel « het bestrijden van onrecht en van elke willekeurige inbreuk op de rechten van een individu of een gemeenschap. Zij verdedigt de beginselen van gelijkheid, vrijheid, solidariteit en humanisme waarop de democratische samenlevingen zijn gegrondvest en die zijn afgekondigd onder meer door de Belgische Grondwet [en] het Europees Verdrag voor de Rechten van de Mens [...] ».

Het maatschappelijk doel van tweede verzoekster omvat o.a. de bescherming van het recht op een eerlijk proces, het recht van verdediging, de persoonlijke vrijheid, van het gelijkheidsbeginsel en van het wettigheidsbeginsel in strafzaken. Het maatschappelijk doel van tweede verzoekster kan door de bestreden beslissing worden geraakt en tweede verzoekster heeft derhalve belang bij haar tussenkomst.

10.

Tweede verzoekster kan evenzeer verwijzen naar de hiervoor ten voordele van eerste verzoekster aangehaalde rechtspraak van Uw Hof die bevestigt dat zij het vereiste belang heeft om een beroep tot nietigverklaring of een vordering tot schorsing in te stellen, dan wel in een zaak tussen te komen.

11.

Tweede verzoekster legt een uittreksel over uit de notulen van de vergadering van 21 februari 2014 waarin haar Raad van Bestuur beslist om het beroep tot vernietiging in te stellen en advocaat Raf Jespers hiertoe mandateer (stuk 6).

De Raad van Bestuur is overeenkomstig artikel 13 van de Wet betreffende de verenigingen zonder winstoogmerk, de internationale verenigingen zonder winstoogmerk en de stichtingen bevoegd om deze beslissing te nemen.

Het beroep tot vernietiging is ontvankelijk.

B. Ontvankelijkheid wat de termijnen betreft

12.

Het beroep tot vernietiging van de bestreden is ingesteld binnen de zes maanden na de bekendmaking van de bestreden wet overeenkomstig artikel 3,§1 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, zijnde 23 augustus 2013, en uiterlijk op de overeenkomstig artikel 119 van diezelfde wet verplaatste vervaldag.

Het beroep tot vernietiging van de bestreden wet is ontvankelijk wat de termijn betreft.

III. In feite – de achtergrond van de bestreden wet

13.

De bestreden wet zet 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 en tot wijziging van Richtlijn 2002/58/EG ("Databewaringsrichtlijn") (Publicatieblad, 13 april 2006, L 105/54) en artikel 15.1 van 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") (Publicatieblad, 31 juli 2002, L 201/37) ("Richtlijn betreffende privacy en elektronische communicatie) gedeeltelijk om in Belgisch recht.

Voorafgaandelijk aan de uiteenzetting van de eigenlijke middelen geven verzoekers hierna een samenvatting van de Europese Databewaringsrichtlijn en diens impact op artikel 8 EVRM, gevolgd door een overzicht van de hangende procedure voor het Europees Hof voor Justitie (EHJ), alsook enkele rechtsvergelijkende gegevens.

A. Artikel 8 EVRM, artikel 22 G.W., artikel 7, 8, 11 en 52.1 Handvest

14.

Dit zijn de basisartikels waarover de discussie voor uw Hof gaat.

Artikel 8 EVRM beschermt het recht op privacy en het communicatiegeheim:

> Recht op eerbiediging van privé-, familie- en gezinsleven
>
> *1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*
>
> *2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.*

Artikel 22 G.W.:

> *Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaalt.*

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

Artikel 7 Handvest:

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

Artikel 8 Handvest:

1. *Eenieder heeft recht op de 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 er op toe dat deze regels worden nageleefd.*

Artikel 11.1 Handvest:

Eenieder heeft het recht op vrije 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.

Artikel 52.1 Handvest:

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 inachtname 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.

15.

Er wordt aanvaard dat de vermelde artikels 8 EVRM, 22 G.W. en 7 Handvest eenzelfde inhoud hebben.

B. De Europese Dataretentierichtlijn 2006/24/EG

16.

De algemene bewaarplicht van tele-en internetcommunicatiegegevens, die de bestreden wet invoert, vloeit voort uit een Europese richtlijn die de Belgische regering normaliter moest omzetten naar nationaal recht tegen 15 maart 2009.

Het gaat om richtlijn 2006/24/EG "*betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbare beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG*"[2] (Databewaringsrichtlijn).

De databewaringsrichtlijn werd op 21 februari 2006 aangenomen door de Raad in de onmiddellijke nasleep van de terreuraanslag die in Londen op 7 juli 2005 plaatsvond in een aantal metrostations en bussen. Deze verregaande richtlijn werd publiek dan ook gerechtvaardigd vanuit een strijd tegen de terreur, maar de vraag naar één of andere vorm van bewaarplicht bestond al veel langer. Zo circuleerden er al sinds het einde van de jaren 1990 wenslijstjes van politiediensten over de omvang en inhoud van een bewaarplicht. Besluitvorming ter zake bleef lange tijd uit gezien de mensenrechtelijke impact, maar het wetgevend proces kwam in een stroomversnelling door de publieke verontwaardiging over de verschillende terreuraanslagen op Westerse bodem in New York, Madrid en Londen.

De databewaringsrichtlijn werd in het leven geroepen om telecomoperatoren en internetproviders te verplichten bepaalde gegevens die door hen gegenereerd of verwerkt worden te bewaren. Op deze manier willen de Europese Commissie en de Raad van de Europese Unie garanderen dat dergelijke gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van 'ernstige criminaliteit', zonder evenwel de draagwijdte van dit begrip nauwkeurig te omschrijven.

Het gaat meer bepaald om alle gegevens betreffende de betrokken personen, de datum, het tijdstip, de duur en de omvang van een telefoongesprek, een SMS-, of e-mailbericht, alsook de gebruikte technologie en de locatie ervan. Het doel is te weten wie met wie, wanneer, voor hoe lang, en van waar gebeld, ge-sms't, of ge-e-maild heeft.

Daarnaast moeten ook de gegevens inzake de toegang tot het internet worden bewaard; bijvoorbeeld wanneer en van op welke computer (en dus vanuit welke plaats) u in-of uitlogde op het internet. Een belangrijke beperking is dat gegevens waaruit de inhoud van de communicatie kan worden achterhaald niet mogen worden bewaard. Dit is een relatief theoretisch onderscheid. Het is perfect mogelijk om via de stelselmatige kennisname van verkeers-en locatiegegevens een min of meer volledig beeld te krijgen van bepaalde aspecten van iemands leven en dus bij deductie van de inhoud van de communicatie.[3] De Belgische 'Fortis-zaak' illustreerde dit. Bijgevolg verdienen deze gegevens een afdoend beschermingsniveau.

Een algemene bewaarplicht van telecommunicatiegegevens perkt de fundamentele rechten van burgers (zoals het recht op privacy en het vermoeden van onschuld) op een significante wijze in.

[2] 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 en tot wijziging van Richtlijn 2002/58/EG [Officieel Publicatieblad L 105 van 13/04/2006 blz. 54-63].

[3] P. Breyer, Submission concerning the action brought on 6 July 2006 Ireland v. Council of the European Union, European Parliament, Case C-301/06, 8 april 2008, p. 6-7.

17.

De databewaringsrichtlijn had in principe tegen 15 september 2007 moeten omgezet zijn, met uitzondering van wat betrekking heeft op de bewaring van communicatiegegevens in verband met internettoegang, internettelefonie en mail via internet, waarvoor de streefdatum voor omzetting was vastgesteld op 15 maart 2009, omdat België gebruik had gemaakt van de in de richtlijn opgenomen mogelijkheid om uitstel te vragen.

In België bleef het lang stil rond de databewaringsrichtlijn, maar eind september 2012 heeft de Europese Commissie België in gebreke gesteld om de richtlijn om te zetten – onder dreiging van geldboetes door het Hof van Justitie. Daarop besliste de regering om met hoogdringendheid vooruit te gaan met de omzetting van deze richtlijn naar intern recht. Diezelfde hoogdringendheid was meteen ook de reden waarom weinig of geen stakeholders werden bevraagd of bij het wetgevend proces werden betrokken.

C. Procedure voor het Europees Hof van Justitie

Feitelijke gegevens

18.

Er kwam uit verschillende hoeken verzet tegen de databewaringsrichtlijn; zij het om verschillende redenen. Zo diende Ierland op 11 juli 2006, later bijgetreden door Slovenië, een verzoek tot vernietiging van de databewaringsrichtlijn in bij het Europese Hof van Justitie (zaak C-301/06).

Ierland was niet op de eerste plaats gekant tegen het principe van een algemene bewaarplicht, maar was van oordeel dat de bewaarplicht op een foutieve rechtsgrond stoelde. Zo oordeelde de Ierse regering dat een bewaarplicht door middel van een kaderbesluit had moeten worden aangenomen binnen het beleidsdomein Justitie en Binnenlandse Zaken, de zogenaamde derde pijler, aangezien de richtlijn tot doel heeft ernstige criminaliteit te bestrijden.

Een van de argumenten van Ierland was de redenering dat vele landen aanvankelijk geen databewaringsregime kenden en dat "*geen enkele kwestie gerelateerd aan de interne markt kon rechtvaardigen dat een lidstaat verplicht werd telecomoperatoren gegevens te laten bijhouden […] indien dergelijke verplichtingen voorheen nog niet bestonden onder de wetgeving van de lidstaat in kwestie*".

Ierland riep toen echter geen mensenrechtelijke bezwaren in tegen deze richtlijn bij haar procedure voor het Europese Hof van Justitie. Door een uitspraak in 2010 van het Ierse Grondwettelijke Hof, zal Ierland in een volgende zaak in 2012 wel mensenrechtelijke bezwaren inroepen (zie infra).

Naar aanleiding van deze eerste procedure door Ierland voor het Europese Hof van Justitie, schaarde zich op 8 april 2008 een grote en diverse groep van organisaties (waaronder burgerrechtenorganisaties, beroepsverenigingen, internetproviders,…) als *'friends of the Court'* achter dit Ierse verzoek tot vernietiging door bijkomende mensenrechtelijke argumenten in te roepen.

Zij oordeelden immers dat naast de discussie of de databewaringsrichtlijn wel op basis van de juiste rechtsgrond was aangenomen, het Hof zich ook best zou uitspreken over een veel belangrijker aspect, namelijk of de databewaringsrichtlijn al dan niet in strijd was met het Europees Verdrag voor de Rechten van de Mens, en meer bepaald met artikel 8 dat het recht op privacy moet vrijwaren.

In haar arrest van 10 februari 2009 oordeelde het Europese Hof van Justitie evenwel dat de databewaringsrichtlijn binnen de eerste pijler moest worden aangenomen aangezien de richtlijn de verplichtingen ten aanzien van telecomoperatoren en internetproviders regelt en niet zozeer het gebruik van deze gegevens door politie en justitie.

Bovendien stelde het Hof dat aangezien de richtlijn terecht binnen de eerste pijler (m.b.t. harmonisatie van de interne markt) was aangenomen en nagenoeg geen bepalingen invoerde ten aanzien van de toegang tot, en het gebruik van, deze gegevens door politie en justitie, men ook geen uitspraak moest doen over het feit of deze richtlijn al dan niet in strijd is met het recht op privacy.

Het Europese Hof van Justitie werd een tweede maal geïnterpelleerd om zich uit te spreken over de grond van de zaak, met name de schending van fundamentele mensenrechten, op basis van een prejudiciële vraag van het Ierse Grondwettelijk Hof.

Het Ierse Grondwettelijk Hof (High Court) stelde in haar arrest van 5 mei 2010 Digital Rights Ireland in het gelijk en in diezelfde maand werd door Ierland een prejudiciële vraag gesteld aan het Europese Hof van Justitie over de schending van de fundamentele mensenrechten door de databewaringsrichtlijn.

Ook het Oostenrijkse Verfassungsgerichtshof stelde gelijkaardige prejudiciële vragen aan het EHJ.

Beide zaken werden gevoegd.

Op 12 december 2013 werd in de samengevoegde zaken een advies uitgebracht door advocaat-generaal P. Cruz Villalon.

De uitspraak van het EHJ wordt in april 2014 verwacht.

Het advies van de advocaat-generaal

19.

Op 12 december 2013 heeft de advocaat generaal bij het Europees hof van Justitie geoordeeld dat de databewaringsrichtlijn incompatibel is met het Handvest Grondrechten van de Europese Unie.[4] Het advies is op zich bijzonder waardevol en ook gezien het latere arrest van het Europees Hof er doorgaans een weerspiegeling van is.

Het advies wordt integraal in de Nederlandstalige versie in de stukken gevoegd. (stuk 6). Verzoekers citeren het advies uitvoerig in het eerste middel.

Meer concreet verwijst het advies naar het algemene artikel 52.1 van het Handvest. Er wordt gesteld dat de databewaringsrichtlijn een onaanvaardbare beperking inhoudt van de uitoefening van de vrijheden die in het Handvest staan.

De beperking die de databewaringsrichtlijn doorvoert met betrekking tot de privacy is niet aanvaardbaar. Concreet bekritiseert het advies dat er in de databewaringsrichtlijn geen voldoende regeling aanwezig is voor garanties inzake de bewaring, de toegang en het gebruik van ingezamelde en weerhouden data. Het advies onderstreept het gevaar voor willekeur en het gebrek aan beschermingsgaranties.
Het advies zet de databewaringsrichtlijn op de helling en stelt dat deze in haar geheel niet in overeenstemming is met artikel 52.1 van het Handvest.

Ten tweede bekritiseert het advies dat de periode voor het bewaren van de data (maximum twee jaar) zoals in de databewaringsrichtlijn opgenomen, veel te lang is.

D. Rechtsvergelijkende gegevens

1. Algemeen

30.

Intussen hebben nationale gerechtshoven in verschillende Europese lidstaten zich reeds moeten uitspreken, of zullen dat in de nabije toekomst moeten doen, over de omzetting van de databewaringsrichtlijn na klachten van burgers, burgerrechtenorganisaties en telecomoperatoren die aanvoeren dat de willekeurige opslag van communicatiegegevens een schending uitmaakt van het fundamentele recht op privacy.

Tal van nationale omzettingswetten werden onderworpen aan een toetsing door respectievelijk de administratieve en grondwettelijke hoven. Deze uitspraken waren vaak vernietigend.

[4] Hof van Justitie van de Europese Unie, Opinie van Advocaat-Generaal Cruz Villalon, 12 december 2013, C-293/12 en C-594/12

Een rechtsvergelijkend overzicht van de meest in het oog springende uitspraken verduidelijkt de voornaamste kritieken tegen een allesomvattende bewaarplicht. Voorts zijn er op datum van indiening van dit verzoekschrift nog zaken hangende in Hongarije, Slovenië, Slovakije en Polen.

Op dit punt moet worden benadrukt dat de omzetting van richtlijn 2006/24 in de verschillende lidstaten niet zonder problemen is verlopen en nog steeds in verschillende mate problemen opwerpt.[5]

2. *Bulgarije*

31.

Een eerste uitspraak met betrekking tot de wetmatigheid van een nationale omzettingswet inzake databewaring kwam er van het Bulgaarse administratieve Hof op vraag van de NGO *Acces to Information Program*. Op 11 december 2008 werd een passage uit de Bulgaarse omzettingswet vernietigd die de Minister van Binnenlandse Zaken indirecte toegang gaf tot de bewaarde data, alsook aan veiligheidsdiensten en andere wetshandhavingsinstanties, zonder gerechtelijk bevel.

"The provision did not set any limitations with regard to the data access by a computer terminal and did not provide for any guarantees for the protection of the right to privacy stipulated by art. 32, para. 1 of the Bulgarian Constitution. No mechanism was established for the respect of the constitutionally granted right of protection against unlawful interference in one's private or family affairs and against encroachments on one's honour, dignity and reputation."[6]

Eigen vertaling:
"De wetsbepaling voert geen beperkingen in met betrekking tot de toegang tot data in computers en voorziet geen enkele garantie voor de bescherming van het recht op privacy vastgelegd in artikel 32, § 1 van de Bulgaarse grondwet. Er is geen mechanisme voorzien voor het respect voor het grondwettelijk beschermd recht van bescherming tegen onwettige inmenging in het privé leven of in familiezaken en tegen het binnendringen in de eer, de waardigheid en de reputatie van een persoon".

Het Hof oordeelde bovendien dat de nationale omzettingswet te weinig refereerde naar andere relevante wetgeving die het gebruik van en de toegang tot de data reglementeert.

---

[5] Zoals blijkt uit beslissingen die zijn gewezen door het Curtea Constituțională (Roemeens Gondwettelijk Hof, zie beslissing van 8 oktober 2009, nr. 1.258; zie voor een vertaling in het Engels http://www.ccr.ro/files/products/D1258_091.pdf), het Bundesverfassungsgericht (Duits Grondwettelijk Hof (zie beslissing van 2 maart 2010, reeds aangehaald), het Ústavní Soud (Tsjechisch Grondwettelijk Hof, zie arrest van 22 maart 2011, Pl. ÚS 24/10;), het Varhoven administrativen sad (Hoogste administratieve gerecht van Bulgarije, beslissing van 11 december 2008, nr. 13627) of ook van het Anotato Dikastirio tis Kypriakis Dimokratias (Cypriotisch Hooggerechtshof, beslissing van 1 februari 2011, n° 183(I)/2007). Bij het Alkotmánybíróság (Hongaars Grondwettelijk Hof) zou beroep zijn ingesteld (zie „Hungarian Data Retention Law - Challenged at the Constitutional Court", EDRI-Gram nr. 6.11, 4 juni 2008), een ander beroep zou aanhangig zijn bij het Ustavno sodišče (Sloveens Grondwettelijk Hof, zie „Slovenia: Information Commissioner challenges the Data Retention Law", EDRI-Gram nr. 11.6, 27 March, 2013).
Zie ook arresten van 9 maart 2010, Commissie/Duitsland (C-518/07, Jurispr. blz. I-1885); 16 oktober 2012, Commissie/Oostenrijk (C-614/10, nog niet gepubliceerd in de Jurisprudentie); zie tevens in een breder verband, arresten van 20 mei 2003, Österreichischer Rundfunk e.a. (C-465/00, C-138/01 en C-139/01, Jurispr. blz. I-4989); 6 november 2003, Lindqvist (C-101/01, Jurispr. blz. I-12971); 16 december 2008, Huber (C-524/06, Jurispr. blz. I-9705) en Satakunnan Markkinapörssi en Satamedia (C-73/07, Jurispr. blz. I-9831); 7 mei 2009, Rijkeboer (C-553/07, Jurispr. blz. I-3889); 9 november 2010, Volker und Markus Schecke en Eifert (C-92/09 en C-93/09, Jurispr. blz. I-11063); 24 november 2011, Scarlet Extended (C-70/10, Jurispr. blz. I-11959) en ASNEF en FECEMD (C-468/10 en C-469/10, Jurispr. blz. I-12181), alsmede 30 mei 2013, Worten (C-342/12, nog niet gepubliceerd in de Jurisprudentie).
[6] http://www.aip-bg.org/documents/data_retention_campaign_11122008e...

"National legal norms shall comply with that established principle [limitations on rights permitted by Article 8(2) of the European Convention of Human Rights] and shall introduce comprehensible and well formulated grounds for both access to the personal data of citizens and the procedures for their retention. Article 5 of the Regulation lacks clarity in terms of protection of the right of private and family life which contradicts the provision of Article 8 of the ECHR, the texts of the Directive 2006/24/EC and articles 32 and 34 of the Bulgarian Constitution."

Eigen vertaling:
"Nationale wetten moeten overeenstemmen met het principe van beperkingen van de rechten zoals bepaald in artikel 8(2) EVRM en moet duidelijke en precies geformuleerde gronden invoeren zowel voor de toegang tot persoonlijke data van burgers als voor de procedure om deze data te bewaren. Artikel 5 van de wet ontbeert duidelijk wat betreft de termen waarin de bescherming van het privé- en familieleven is geformuleerd wat in strijd is met artikel 8 EVRM, de tekst van richtlijn 2006/24/EG en de artikels 32 en 34 van de Bulgaarse grondwet."

3. Cyprus

32.

In februari 2011 vernietigde het Cypriotische Hooggerechtshof bepalingen van de nationale omzettingswet 183(I)2007 wegens strijdigheid met artikel 15.1 (recht op privacy en familie- en gezinsleven) en artikel 17.1 (geheimhouding van communicatie) van de Grondwet.[7]

4. Duitsland

33.

Het Bundesverfassungsgericht in Duitsland vernietigde de Duitse implementatiewetten op grond van een foutieve interpretatie van de Europese Richtlijn.[8] De Duitse implementatiewet (Telekommunikationsgesetz) werd bovendien strijdig bevonden met artikel 10 van de Duitse Grondwet (Grundgesetz) en met het recht op privacy, meer bepaald met de veiligheid en integriteit van telefonische- en postcommunicatie.

Zo is er het arrest van 2 maart 2010 van het Federale Grondwettelijk Hof van Duitsland waarin wordt gesteld dat de algemene bewaarplicht een grote beperking inhoudt van het recht op privacy en daarom enkel onder beperkte omstandigheden mag worden toegepast.

Een databewaringsperiode van zes maanden is, volgens het Duitse Hof, de absolute bovengrens van wat als proportioneel kan worden beschouwd (paragraaf 215). Verder stelt het Duitse Hof dat data enkel mogen worden opgevraagd indien er reeds een vermoeden was van een ernstig misdrijf of bewijs van een gevaar voor de openbare veiligheid.

[7] Hooggerechtshof Cyprus, 65/2009, 78/2009, 82/2009 en 15/2010-22/2010, http://www.supremecourt.gov.cy/Judicial/SC.nsf/All/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf
[8] BVerfG, 1 BvR 256/08, 2 maart 2010, Absatz-Nr. (1 - 345), http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

Ook moet het opvragen van data worden verboden in bepaalde gevallen (bijvoorbeeld data inzake emotionele of sociale zaken) die gebaseerd zijn op vertrouwelijkheid. Er moet een transparant overzicht plaatsvinden van gebruik van data.

Het Bundesverfassungsgericht oordeelde dat:

"the protection of communication does not include only the content but also the secrecy of the circumstances of the communication, including especially if, when and how many times did some person (...) contact another or tried that".

Eigen vertaling:
"De bescherming van de communicatie mag niet enkel de inhoud insluiten maar ook de geheimhouding van de omstandigheden van de communicatie, met inbegrip in het bijzonder, wanneer en hoeveel keer een persoon … een ander contacteerde of trachtte te contacteren."

Zich baserend op een privacy-test, gelijkaardig aan deze ontwikkeld binnen het EHRM, oordeelde het Bundesverfassungsgericht dat een bewaartermijn van 6 maanden enkel in uitzonderlijke omstandigheden gerechtvaardigd kan zijn en dat preventieve gegevensverzameling aanleiding kan geven tot een gevoel van permanente controle.

De Duitse implementatiewet voldeed niet aan de grondwettelijke vereiste van proportionaliteit wat betreft doelbinding, gegevensbeveiliging, transparantie en controle tegen misbruik. Het Hof laakte de gebrekkige reglementering van de toegang tot de data en het gebrek aan voldoende veiligheidsgaranties.

Nog volgens het Duitse Hof verdienen ook locatie- en verkeersdata voldoende bescherming, daar hun verwerking belangrijke, zelfs gevoelige, persoonlijke gegevens kan blootleggen. Het Hof stond ook stil bij het gevoel van onbehangen dat een allesomvattende bewaarplicht kan genereren:

" a preventive general retention of all telecommunications traffic data (...) is also to be considered as such a heavy infringement because it can evoke a sense of being watched permanently (...). The individual does not know which state official knows what about him or her, but the individual does know that it is very possible that the official does know a lot, possibly also highly intimate matter about him or her" (§241).

Eigen vertaling:
"een preventieve algemene bewaring van alle verkeersgegevens van telecommunicatie … moet ook als dusdanig beschouwd worden als een ernstige inbreuk omdat dit een gevoel van permanent bewaakt te worden kan oproepen … De individuele burger zal niet weten welke officiële staatsbeambte wat over hem of haar weet, maar hij zal wel weten dat het zeer goed mogelijk is dat die officiële persoon heel wat over hem of haar weet, mogelijk ook zeer intieme gegevens."

5. Roemenië

34.

Het Grondwettelijk Hof van Roemenië oordeelde in oktober 2009 tot de ongrondwettigheid van omzettingswet 298/2008, op grond van een schending van het recht op bewegingsvrijheid, het recht op de eerbiediging van de persoonlijke levenssfeer en een schending van het briefgeheim en de vrijheid van meningsuiting, die niet in overeenstemming is met de restricties toegelaten in de Roemeense Grondwet (artikel 53).[9]

"The obligation to retain the data, established by Law 298/2008, as an exception or a derogation from the principle of personal data protection and their confidentiality, empties through its nature, length and application domain, the content of this principle."

Eigen vertaling:
"De verplichting om data te bewaren, zoals vastgelegd in de wet 298/2008, als een uitzondering op of een afwijking van het principe van bescherming en vertrouwelijkheid van persoonsgegevens, maakt door haar natuur, de duur en het toepassingsterrein een lege doos van die principes."

Het Roemeense Grondwettelijk Hof beschouwt het gebrek aan een precieze wettelijke bepaling omtrent de noodzakelijkheid van de gegevens in het licht van de identificatie van de gebruikers als een mogelijkheid tot misbruik in hoofde van de dienstverleners.

Het Hof acht de Roemeense wet op een al te dubbelzinnige wijze opgesteld wegens een gebrek aan duidelijk afgelijnde begrippen (o.a. het vage "bedreigingen van de nationale veiligheid"), alsook aan transparantie ten aanzien van onwetende burgers die zich verdacht maken als gevolg van bepaalde gedragingen. Ook de toegang tot de data is onzorgvuldig geregeld.
Het Hof refereert naar relevante rechtspraak van het Europees Hof waarin wordt gesteld dat "*taking surveillance measures without adequate and sufficient safeguards can lead to 'destroying democracy on the ground of defending it'*" (*Klass v Germany,* 1978[10]).

Eigen vertaling:
"het nemen an controle maatregelen zonder adequate en afdoende beschermingsmechanismen kan leiden tot de vernietiging van de democratie onder de vlag van de verdediging ervan".

Het Roemeense Hof wijst bovendien ook op het voortdurend karakter van de bewaarplicht, hoewel het recht op persoonlijke levenssfeer een onthoudingsplicht ten aanzien van overheidsdiensten lijkt te impliceren, waarbij een inbreuk op het fundamentele recht op privacy tot een strikt minimum moet worden beperkt (Cfr. Richtlijn 2002/58/EC).

[9] Roemenië, Grondwettelijk Hof, 8 oktober 2009, no.1258, http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf
[10] Europees Hof voor de Rechten van de Mens, Klass and others v Germany, 6 september 1978, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-57510#{%22itemid%22:[%22001-57510%22]}

"The limitation of exerting the right to private life and to the secrecy of correspondence and the freedom of expression, must also be made in a clear, predictable and unambiguous manner, so that the possibility of the arbitrariness or abuse from authorities in this field may be avoided, as much as possible." […]
"The legal obligation that foresees the continuous retention of personal data transforms though the exception from the principle of effective protection of privacy right and freedom of expression, into an absolute rule."

Eigen vertaling:
"De beperking van de uitoefening van het recht op privéleven, het briefgeheim en de vrijheid van meningsuiting, moet ook geschieden op een duidelijke, voorzienbare en ondubbelzinnige manier, zodat de mogelijkheid van willekeur of misbruik door de overheden op dit terrein zo veel als mogelijk vermeden wordt."
"De wettelijke verplichting die het permanent bewaren van persoonsgegevens invoert maakat van de uitzondering van het principe van effectieve bescherming van de privacy en van de meningsvrijheid, een absolute regel".

6. Tsjechië

35.

Het Grondwettelijk Hof van de Tsjechische Republiek sprak zich, in maart 2011, uit over de ongrondwettigheid van de Wet op Elektronische Communicatie 127/2005 op grond van een schending van het fundamentele recht op privacy, meer bepaald het recht op informationele zelfbeschikking, in het licht van het beginsel van proportionaliteit.[11]

Het Hof oordeelde dat de bewaartermijn, opgelegd door de nationale omzettingswet, de maximumtermijnen uit de Richtlijn overschrijdt en dat het gebruik van de bewaarde gegevens zich niet beperkt tot situaties van zware criminaliteit en terrorisme. De Tsjechische omzettingswet werd ook een gebrek aan beschermingsmaatregelen en transparantie verweten. In een tweede uitspraak datzelfde jaar vernietigde het Hof de vage toegangsprocedures die disproportioneel werden bevonden in het licht van het recht op privacy en informationele zelfbeschikking.

E. De evaluatie door de Europese Commissie van de Richtlijn 2006/24/EG

36.

Dat de richtlijn 2006/24/EG erg problematisch is en was blijkt ten overvloede, maar niet enkel, uit de hierboven geciteerde vernietigingen van implementatiewetten van de Grondwettelijke

[11] De Tsjechische Republiek, Grondwettelijk Hof, 22 maart 2011, Pl. US 24/10, 94/11 Coll., http://www.edri.org/files/DataRetention_Judgment_ConstitutionalCourt_CzechRepublic.pdf

Hoven in diverse landen en van de thans nog lopende procedures én voor enkele Grondwettelijke Hoven en voor het Europees Hof van Justitie.

Er is ook zeer veel protest van mensenrechtenorganisaties en burgers in alle EU-landen. Zij maken zich effectief zorgen dat met deze richtlijn en de omzetting ervan een onaanvaardbare grens overschreden wordt op het vlak van aantasting van de fundamentele rechten en vrijheden. In Duitsland werd de procedure voor het Grondwettelijk Hof bij petitie ondersteund door 35.000 burgers, in Oostenrijk door 11.130 burgers.

De Europese Commissie zag zich verplicht in 2011 een evaluatie te maken.
In het eindrapport worden volgende besluiten geformuleerd:[12]

-de EU zal zijn ondersteuning geven bij en ervoor zorgen dat de dataretentie als een maatregel van veiligheid zal beschouwd worden, in tegenstelling tot de richtlijn die als een zaak van regeling van de interne markt werd opgevat;

-de omzetting van de richtlijn in de verschillende EU-landen is 'hoog problematisch'.

-de richtlijn is er niet in geslaagd de benadering van databewaring volledig te harmoniseren en heeft geen draagvlak gecreëerd voor de operators;

-de operators moeten wezenlijk vergoed worden voor hun bijkomende kosten;

-verdere databewaring moet het principe van proportionaliteit respecteren en mag niet verder gaan dan wat nodig is om ernstige criminaliteit en terrorisme te bestrijden. In dat verband worden dan concrete maatregelen voorgesteld zoals: beperken van de doelstellingen en het vastleggen van welbepaalde vormen van criminaliteit voor databewaring; verkorting van de periodes van bewering; instelling van een onafhankelijke toezichthouder; beperking van de overheden die toegang hebben tot de data; herleiden van de te bewaren datacategorieën; …

Als algemene conclusie wordt 'de herziening van de huidige richtlijn' vooropgesteld, en dit na raadpleging van de juridische wereld, de industrie, consumentengroepen, databeschermingsautoriteiten en organisaties van de burgerlijke samenleving.

De kritieken op de richtlijn zijn wezenlijk.
Ondanks de in april 2011 het vooruitzicht gestelde herziening is deze op datum van het indienen van dit verzoekschrift nog steeds in de EU-ijskast.

Dit gegeven en inzonderheid de inhoud van de eigen evaluatie door de Commissie zou op zich moeten hebben volstaan voor de Belgische wetgever om, minstens in afwachting van de herziening, geen wet te maken. Het tegendeel gebeurde.

Nochtans hebben landen zoals Duitsland tot op vandaag geweigerd de wet (opnieuw) te implementeren.

[12] European Commission, Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/21/EC), 18.4.2011, COM(2011) 225 final, pp. 30-33.

F. De Belgische dataretentiewet

37.

De omzetting van de dataretentierichtlijn gebeurde deels aan de hand van een wijziging van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie en deels door aanneming van een koninklijk besluit ter uitvoering van dat nieuwe artikel 126, zodat de lijst van te bewaren gegevens en de vereisten waaraan deze gegevens moeten beantwoorden zullen worden vastgelegd door de Koning.

Ondanks het gegeven dat de richtlijn dateert van 2006 kende het wetsontwerp Vande Lanotte – Turtelboom, dat uiteindelijk zal leiden tot de hier bestreden wet, een merkwaardig wetgevend parcours.

Het wetsontwerp werd bij de Kamer ingediend op 27.6.2013. Het bekwam op 4.7.2013 de urgentie. Het werd op 9.7.2013 besproken in de commissie infrastructuur, verkeer en overheidsbedrijven van de Kamer. De algemene vergadering van de Kamer nam het aan op 17.7.2013. Het werd geëvoceerd door de Senaat, niet geamendeerd, behandeld door de commissie economie, en gestemd door de algemene vergadering op 18.7.2013.

Ondanks verzoeken van parlementsleden en vanuit onder meer verzoekers werden er geen experts gehoord of hoorzittingen gehouden.

Dit voor de mensenrechten ingrijpend wetsontwerp werd in volle verlofperiode op een termijn van 21 dagen ingediend en gestemd, zonder noemenswaardig debat in de commissies of in de plenaire vergaderingen van de twee Kamers. Het wetsontwerp werd niet voorgelegd aan de commissies Justitie van beide kamers, hoewel het wetsontwerp wezenlijk raakt aan een materie die tot de bevoegdheid van deze commissies behoort en het mede werd ingediend door de minister van Justitie zelf. Het ging om een wetsontwerp waarvoor België reeds sedert 2006 de mogelijkheid had om het om te zetten. Vermelde snelle en ongewone gang van behandeling in een zo'n belangrijke mensenrechtenmaterie is volgens verzoekers problematisch in een parlementaire democratie.

38.

Het ontwerp van wet werd tweemaal voorgelegd aan de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (hierna: Privacycommissie) (in 2008[13] en 2009[14]). In haar nr. 20/2009 geeft de Privacycommissie een gunstig advies over het voorontwerp van wet en het ontwerp van koninklijk besluit, op voorwaarde dat rekening wordt gehouden met bepaalde opmerkingen.

[13] Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Advies nr. 24/2008 van 2 juli 2008.
[14] Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Advies nr. 20/2009 van 1 juli 2009.

De bestreden wet heeft echter maar op een aantal punten rekening gehouden met het advies van de Privacycommissie. Wat betreft bestreden wet van 30 juli 2013 werd de Privacycommissie zelfs niet meer bij het omzettingsproces betrokken.
De adviezen van de Privacycommissie dateren bijgevolg van een periode voordat diverse Grondwettelijke Hoven en de Europese Commissie zelf, vernietigende uitspraken en kritieken op de richtlijn 2006/24 hebben gemaakt, en zijn bijgevolg erg relatief.

39.

Ook de Raad van State werd in de mogelijkheid gesteld een advies uit te brengen, dat slechts beperkt door de wetgever werd gevolgd.[15]

De Raad van State kritiseert het wetsontwerp onder meer op volgende punten:

- De Raad van State verwijst uitdrukkelijk naar het evaluatierapport van de Europese Commissie en op een aantal kritische punten uit dit rapport die in het wetsontwerp niet worden weerlegd: het begrip 'ernstige criminaliteit' als uitgangspunt (wet hanteert zelfs dit begrip niet, maar enkel 'strafbare feiten'); het gebrek aan harmonisatie op EU-vlak; de onvoldoende mate van voorspelbaarheid van het opvragen van de bewaarde data, …

- De tweedeling tussen RL 2006/24/EG en RL 2002/58/EG. De Raad van State stelt dat het niet opgaat de twee richtlijnen, die een andere doelstelling hebben, via éénzelfde wetsinstrument om te zetten. Het stelt dat het gaat om een 'ingewikkeld juridisch verband' en vraagt zich af of de beste oplossing om te garanderen dat het Europees recht wordt nageleefd er niet in bestaat twee naast elkaar bestaande regelingen op te zetten. 'Hoe het ook zij, daar de steller van het voorontwerp heeft gekozen voor een regeling die op de twee voornoemde richtlijnen steunt, moet hij het tweeledig juridisch kader naleven waarop hij zich beroept'.
  Verzoekers merken u al op dat de bestreden wet niet doet wat de Raad van State stelt dat moet gebeuren.

- De wijze van overdracht en de bevoegde overheidsinstanties (dit laatste betreft artikel 127 § 2, b en c) worden niet verduidelijkt in het wetsontwerp.

- Het invoeren van twee verschillende bewaartermijnen: de Raad van State stelt zich de vraag of in sommige gevallen de termijn van gegevensbewaring niet wordt overschreden.

- De toegang door één of meerdere leden van de Coördinatiecel Justitie tot de bewaarde data; dit moet volgens de Raad van State gewijzigd worden.

- Het begrip 'oproeppoging zonder resultaat' moet gedefinieerd worden.

[15] Raad van State, advies nr. 53.272/4 van 27 mei 2013.

IV. De middelen

Eerste middel

Schending van de artikelen 10, 11, 12, 15, 22 en 29 van de Grondwet, op zichzelf genomen en/of in samenhang met de artikelen 5, 8, 9, 10, 11, 14, 15, 17 en 18 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), met artikel 7, 8, 11 en 52 (1) van het Handvest van de grondrechten van de Europese Unie (HANDVEST), met artikel 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (BUPO), met de algemene rechtsbeginselen van rechtszekerheid, evenredigheid en informationele zelfbeschikking, met artikel 5 §4 van het Verdrag EU.

Geschonden referentienormen – Recht op de eerbiediging van de persoonlijke levenssfeer en bescherming van persoonlijke data, al dan niet in samenhang gelezen met het recht op vertrouwelijkheid van communicatie en de algemene rechtsbeginselen – waaronder het beginsel van de informationele zelfbeschikking en het legaliteits-, evenredigheids- en subsidiariteitsbeginsel:

1.

Aangevochten beschikkingen van de bestreden wet

40.

Artikel 5 van de bestreden wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet betreffende de elektronische communicatie en van artikel 90 decies van het Wetboek van strafvordering bepaalt:

Artikel 126 van dezelfde wet wordt vervangen als volgt:

" Art. 126. § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bewaren de aanbieders van aan het publiek aangeboden vaste telefoniediensten, mobiele telefoniediensten, internettoegangdiensten, internet-e-maildiensten, of internettelefoniediensten, en de aanbieders van de onderliggende openbare elektronische- communicatienetwerken de verkeersgegevens, de locatiegegevens, de gegevens voor identificatie van de eindgebruikers, de gegevens voor identificatie van de gebruikte elektronische-communicatiedienst en de gegevens voor identificatie

van de vermoedelijk gebruikte eindapparatuur, die door hen worden gegenereerd of verwerkt bij het leveren van de betreffende communicatiediensten.

Onder aanbieders in de betekenis van dit artikel worden ook de doorverkopers in eigen naam en voor eigen rekening verstaan.

Onder telefoniedienst in de betekenis van dit artikel wordt verstaan : telefoonoproepen - met inbegrip van spraakoproepen, voicemail, conference call of datacommunicatie-, aanvullende diensten - met inbegrip van call forwarding en call transfer -, en de messaging- en multimediadiensten - met inbegrip van short message service (sms), enhanced media service (EMS) en multimedia service (MMS).

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 krachtens het eerste lid te bewaren gegevens per type dienst alsook de vereisten waaraan deze gegevens moeten beantwoorden.

Behoudens andersluidende wettelijke bepaling, mogen geen gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, bewaard worden.

De verplichting om de in het eerste lid bedoelde gegevens te bewaren, is ook van toepassing op oproeppogingen zonder resultaat, voor zover die gegevens in verband met de aanbieding van de bedoelde communicatiediensten:

1° wat de telefoniegegevens betreft, worden gegenereerd, verwerkt en opgeslagen door de aanbieders van openbare diensten voor elektronische communicatie of van een openbaar netwerk voor elektronische communicatie, of

2° wat de internetgegevens betreft, door deze aanbieders worden gelogd.

§ 2. De gegevens bedoeld in paragraaf 1, eerste lid, worden bewaard met het oog op :

a) de opsporing, het onderzoek en de vervolging van strafbare feiten zoals bedoeld in de artikelen 46bis en 88bis van het Wetboek van strafvordering;

b) de beteugeling van kwaadwillige oproepen naar de nooddiensten, zoals bedoeld in artikel 107;

c) het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of -dienst, zoals bedoeld in artikel 43bis, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

d) de vervulling van de inlichtingenopdrachten met inzet van de methoden voor het verzamelen van gegevens zoals bedoeld in de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de gegevens opgenomen in paragraaf 1, eerste lid, onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en op eenvoudig verzoek aan de autoriteiten belast met de opdrachten bedoeld in de punten a) tot d) kunnen worden meegedeeld en uitsluitend aan deze laatsten.

§ 3. De gegevens ter identificatie van de eindgebruikers, de gebruikte elektronische-communicatiedienst en de vermoedelijk gebruikte eindapparatuur worden bewaard vanaf de inschrijving op de dienst, zolang binnenkomende of uitgaande communicatie mogelijk is door middel van de dienst waarop werd ingetekend en gedurende twaalf maanden vanaf de datum van de laatste geregistreerde binnenkomende of uitgaande communicatie.

De verkeers- en localisatiegegevens worden bewaard gedurende twaalf maanden 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 gegevens die zijn onderworpen aan het eerste lid en deze die zijn onderworpen aan het tweede lid.

§ 4. Naar aanleiding van het evaluatieverslag bedoeld in paragraaf 7, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer, de bewaringstermijn van de gegevens voor bepaalde categorieën van gegevens aanpassen, zonder een termijn van meer dan 18 maanden vast te leggen.

De Koning kan, in de omstandigheden zoals bedoeld in artikel 4, § 1, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Commissie voor de bescherming van de persoonlijke levenssfeer, voor een beperkte periode, een bewaringstermijn voor de gegevens vastleggen die langer is dan twaalf maanden.

Wanneer in de omstandigheden bedoeld in het tweede lid de Koning een bewaringstermijn oplegt die langer is dan vierentwintig maanden, stelt de minister de Europese Commissie en de overige lidstaten van de Europese Unie onverwijld in kennis van alle genomen maatregelen, met vermelding van de redenen die eraan ten grondslag liggen.

§ 5. Voor de bewaring van de in paragraaf 1, eerste lid, bedoelde gegevens geldt het onderstaande voor de aanbieder van een netwerk of dienst voor elektronische communicatie bedoeld in paragraaf 1, eerste lid :

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

2° hij zorgt ervoor 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° hij garandeert dat de toegang tot de bewaarde gegevens enkel gebeurt door een of meer leden van de Coördinatiecel Justitie bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie en door het personeel en de aangestelden van deze aanbieders die specifiek door deze cel gemachtigd zijn;

4° hij zorgt ervoor dat de gegevens na afloop van de bewaringstermijn die voor die gegevens geldt, worden vernietigd.

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 technische en administratieve maatregelen die de aanbieders van diensten en netwerken beoogd in paragraaf 1, eerste lid, moeten nemen teneinde de bescherming van de bewaarde persoonsgegevens te garanderen.

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, worden beschouwd als verantwoordelijk voor de verwerking van deze gegevens in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

§ 6. De minister en de Minister van Justitie zorgen ervoor dat jaarlijks aan de Europese Commissie en de Kamer van volksvertegenwoordigers statistische informatie wordt verstrekt over de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare communicatiediensten of -netwerken. Die informatie heeft onder meer betrekking op :

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 niet konden worden ingewilligd.

Deze statistische informatie mag geen persoonsgegevens omvatten.

De gegevens die betrekking hebben op de toepassing van paragraaf 2, a), worden tevens bijgevoegd bij het verslag dat de Minister van Justitie overeenkomstig artikel 90decies 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 van diensten of netwerken jaarlijks moeten overzenden aan het Instituut en deze die het Instituut overzendt aan de minister en aan de Minister van Justitie.

§ 7. Onverminderd het verslag bedoeld in paragraaf 6, derde lid, brengen de minister en de Minister van Justitie, twee jaar na de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 1, derde lid, aan de Kamer van volksvertegenwoordigers een evaluatieverslag uit 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".

2. Het onderzoekskader

2.1.

Het onderzoekskader volgens de rechtspraak van het EHRM en van het Grondwettelijk Hof

41.

In het arrest nr. 66/2013 van 16 mei 2013 inzake *Liga van belastingplichtigen* en anderen formuleert uw Hof volgende principes met betrekking tot de beoordeling van artikel 22 van de Grondwet:

"B.8.1. Artikel 22 van de Grondwet heeft tot doel de personen te beschermen tegen inmenging in hun privéleven en gezinsleven.
Het Hof moet bijgevolg nagaan of de verplichting voor de financiële instellingen om aan de belastingadministratie briefwisseling vrij te geven die zij met hun cliënten hebben gehad, bestaanbaar is met het recht op eerbiediging van hun privéleven.

B.8.2. Uit de parlementaire voorbereiding van artikel 22 Grondwet blijkt dat de Grondwetgever 'een zo groot mogelijke concordantie heeft willen nastreven met artikel 8 van het Europees Verdrag tot Bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), teneinde betwistingen over de inhoud van dit Grondwetsartikel respectievelijk artikel 8 van het EVRM te vermijden' (Parl. St., Kamer, 1992-1993, nr. 997/5, p. 2).

B.8.3. De rechten die bij artikel 22 en bij artikel 8 EVRM worden gewaarborgd zijn niet absoluut.

B.10. Het Hof moet voorts nagaan of die inmenging voldoet aan het wettigheidsbeginsel en of zij redelijk verantwoord is.

B.11.1. … Naast die formele wettigheidscontrole legt artikel 22 van de Grondwet eveneens de verplichting op dat de inmenging in het recht op eerbiediging van het privéleven in duidelijke en voldoende nauwkeurige bewoordingen wordt geformuleerd die het mogelijk maken de hypothesen te voorzien waarin de wetgever een dergelijke inmenging in het recht op eerbiediging van het privéleven toestaat.

Evenzo houdt de vereiste van voorzienbaarheid waaraan de wet moet voldoen om in overeenstemming te worden bevonden met artikel 8 EVRM, in dat de formulering ervan voldoende precies is zodat elk individu in de gegeven omstandigheden in redelijke mate de gevolgen van een bepaalde handeling kan voorzien (EHRM, 17 februari 2004, *Maestri* t. Italië, § 30).

De wet moet waarborgen bieden tegen willekeurige aantastingen door de overheid van het recht op eerbiediging van het privéleven, namelijk door de beoordelingsbevoegdheid van de betrokken overheden op voldoende duidelijke wijze af te bakenen, enerzijds, en door in een effectief jurisdictioneel toezicht te voorzien, anderzijds (zie, onder andere, EHRM, 4 mei 2000, *Rotaru* t. Roemenië, § 55; 6 juni 2006, *Segerstedt-Wiberg* t. Zweden, § 76; 4 juli 2006, *Lupsa* t. Roemenië, § 34).

B.12. Het Hof moet voorts nagaan of de inmenging in het recht op eerbiediging van het privéleven van de belastingplichtige en van de personen met wie hij financiële verrichtingen heeft gedaan, redelijk is verantwoord. Daartoe dient te worden nagegaan of de motieven die zijn aangevoerd om die inmenging te verantwoorden, relevant en toereikend zijn, alsook of het evenredigheidsbeginsel is nageleefd."

Het verzamelen, vooral het bewaren in gigantische databases van talloze gegevens die zijn gegenereerd of verwerkt in het kader van het grootste deel van de gebruikelijke elektronische communicatie van de burgers vormt een duidelijke inmenging in hun privéleven, ook al worden daarmee enkel de voorwaarden geschapen om achteraf hun activiteiten te controleren. (overweging 72, advocaat-generaal EHJ).

Het Europees Hof voor de Rechten van de Mens heeft meermaals geoordeeld dat het mogelijk noch noodzakelijk is het begrip „privéleven" uitputtend te definiëren; zie met name arrest van 16 december 1992, Niemietz/Duitsland, klacht nr. 13710/88, Serie A, n° 251-B, § 29. Het betreft in ieder geval een „ruim" begrip: zie arrest, van 19 april 2002 Pretty/Verenigd Koninkrijk. Zie over het begrip privéleven met name Rubenfeld, J., „The Right of Privacy", *Harvard Law Review*, 1989, deel 102, blz. 737; De Schutter, O., „La vie privée entre droit de la personnalité et liberté", *Revue trimestrielle des droits de l'homme*, 1999, blz. 827, Wachsmann, P., „Le droit au secret de la vie privé", in Sudre F., „*Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*", Bruylant, 2005, blz. 119, en Rigaux, F., „La protection de la vie privée en Europe", in *Le droit commun de l'Europe et l'avenir de l'enseignement juridique*, van Witte B, en Forder, C. uitg., Metro, Kluwer, 1992, blz. 185.

42.

Het onderzoekskader dat uit deze rechtspraak en die van het EHRM naar voor komt is het volgende:

1. Voldoet de inmenging aan het wettigheidsbeginsel.

   Dit vereist een onderzoek of de regels van inmenging in het privéleven,

-beantwoorden aan een dwingende maatschappelijke behoefte,

-voldoende precies zijn wat betekent dat ze in duidelijke en voldoende nauwkeurige bewoordingen worden geformuleerd die het mogelijk maken hypothesen te voorzien waarin de inmenging wordt toegestaan en dat de formulering voldoende precies is zodat elk individu in de gegeven omstandigheden in redelijke mate de gevolgen van een bepaalde handeling kan voorzien,

-de beoordelingsbevoegdheid van de betrokken overheden op voldoende duidelijke wijze afbakent en in een effectief jurisdictioneel toezicht voorzien, als waarborg tegen willekeurige aantastingen door die overheden;

2. Is de inmenging redelijk verantwoord.

   Dit vereist een onderzoek naar:

   -het gegeven of de aangevoerde motieven de inmenging verantwoorden, of ze relevant en toereikend zijn, en

   -het naleven van het evenredigheids- of proportionaliteitsbeginsel.

3. Is het subsidiariteitsbeginsel nageleefd.

   Dit vereist een onderzoek naar de vraag of hetzelfde doel niet met minder privacy-ingrijpende maatregelen kan bereikt worden.

Verzoekers zullen aantonen dat de hier bestreden wetsartikels niet beantwoorden aan de gestelde voorwaarden.

2.2.

De toetsing door het Grondwettelijk Hof aan internationale en supranationale bepalingen

43.

‘Het Grondwettelijk Hof kan aan internationale en supranationale bepalingen toetsen door ze te relateren aan artikel 10 en 11 G.W. of aan een grondwettelijk grondrecht. In de tweede plaats kan de internationale norm geïntegreerd worden in een norm van intern recht. … Via de artikelen 10 en 11 G.W. toetst het Grondwettelijk Hof ook aan Europees Gemeenschapsrecht. Het Hof wijst er op dat het op die wijze ook de voorrang van het Europese Gemeenschapsrecht verzekert. … Het Grondwettelijk Hof verzekert de naleving van internationaal recht bovendien door internationale bepalingen te integreren in een norm van nationaal recht. Dat gebeurt via een verdragsconforme of richtlijnconforme interpretatie van de voor toetsing voorgelegde wet of van de Belgische referentienorm, of door de rechtspraak van een internationaal rechtscollege zoals het Europees Hof voor de rechten van de mens te integreren in de interpretatie. … .’

(P. Popelier, Procederen voor het Grondwettelijk Hof, Intersentia Antwerpen-Oxford 2008, n° 269, 274, 277 en 278).

Het Hof kan bijgevolg ofwel door relatering met artikel 10 en 11 G.W. en artikel 22 G.W. of door de integratie via artikel 22 Grondwet, de hier bestreden wet toetsen aan de in het advies als geschonden vermelde normen van het EU-recht, met name artikel 5 § 4 van het verdrag EU, artikel 7 en 52 (1) van het Handvest en aan artikel 8 EVRM.

Minstens kan het Hof een prejudiciële vraag stellen aan het Europees Hof van Justitie met betrekking tot de verenigbaarheid van de Richtlijn 2006/24/EG met het Gemeenschapsrecht (zie beschikkend gedeelte).

3.

Grieven

<u>3.1.</u>

De inhoud van het bestreden artikel 5 van de wet van 30 juli 2013

44.

Vermeld artikel 5 voert met artikel 126, §§ 1 tot en met 5 een wettelijke verplichting in als volgt:

-Aanbieders van telefoondiensten en internettoegang worden verplicht om de verkeersgegevens, de locatiegegevens, de gegevens voor identificatie van de eindgebruikers, de gegevens voor identificatie van de gebruikte elektronische-communicatiedienst en de gegevens voor identificatie van de vermoedelijk gebruikte eindapparatuur te bewaren. (artikel 126 § 1)

-Behoudens andersluidende wettelijke bepalingen, mogen geen gegevens bewaard worden waaruit de inhoud van de communicatie kan worden opgemaakt. (artikel 126 § 1)

-De bewaring gebeurt met het oog op vier doeleinden:
a. opsporing, onderzoek en vervolging van strafbare feiten zoals bedoeld in artikel 46bis en 88bis Wetboek van strafvordering;
b. beteugeling van kwaadwillige oproepen;
c. onderzoek door Ombudsdienst voor telecommunicatie naar identiteit van personen die kwaadwillig gebruik maken van een elektronische communicatiewerk of –dienst;
d. vervulling van de inlichtingenopdrachten door Staatsveiligheid en Veiligheid van het Leger met inzet van de methoden bepaald in artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.
(artikel 126 § 2)

-De gegevens moeten onbeperkt toegankelijk zijn voor de aangeduide doeleinden en onverwijld en op eenvoudig verzoek aan de autoriteiten die ze kunnen opvragen worden meegedeeld. (artikel 126 § 2)

-De identificatiegegevens van de gebruikers moeten bewaard worden vanaf intekening en gedurende twaalf maanden na de laatst geregistreerde communicatie. (artikel 126 § 3)

-De verkeers- en locatiegegevens moeten gedurende twaalf maanden vanaf datum communicatie bewaard worden. (artikel 126 § 3)

-Naar aanleiding van de evaluatie van de wet kan de bewaringstermijn worden aangepast tot maximum 18 maanden. (artikel 126 § 4)

-In de omstandigheden voorzien in artikel 4 §1 van de wet elektronische communicatie van 13 juni 2005 (wanneer openbare veiligheid, de volksgezondheid, de openbare orde of de verdediging van het Rijk dit eisen) kan via KB een bewaringstermijn van langer dan twaalf maanden worden bepaald, en zelfs langer dan 24 maanden. (artikel 126 § 4)

-Er worden bepalingen vastgelegd die de kwaliteit van de bewaarde gegevens en de beperkte toegang er toe moeten garanderen. (artikel 126 § 5)

45.

Deze wetsbepaling komt er op neer dat alle communicatiegegevens van alle burgers die gegenereerd worden via een in België gevestigde telecommaatschappij of internetprovider gedurende 12 maanden worden bewaard, en dat de identificatiegegevens van de gebruiker in principe vanaf de inschrijving op de dienst tot twaalf maanden na de laatste communicatie worden bewaard. Dit laatste komt er op neer dat de gebruiker voor in principe onbeperkte tijd geïdentificeerd wordt en deze gegevens voor die onbeperkte tijd worden opgeslagen.

De wetsbepaling heeft voor gevolg dat vier verschillende en erg uiteenlopende instanties op een eenvoudig verzoek de gegevens kunnen opvragen.

Het gaat om een opslag in bulk en zonder enig onderscheid naar gelang de persoon over wie het gaat. Er ligt geen enkel criterium ten grondslag aan deze massale opslag.

Het gaat om een verplichting tot bewaren en het verlenen van toegang voor exploitatie van persoonsdata van communicatie en identificatie van personen van een kwalitatief en kwantitatief karakter zoals nooit voorheen verplicht werd in de Belgische rechtsorde.

46.

Verzoekers stellen dat de aard van de te bewaren en te exploiteren gegevens het fundamenteel recht op privacy van de burgers schendt.

Deze bewaring en exploitatie is in essentie onverenigbaar met artikel 22 van de Belgische grondwet, in samenlezing met artikel 8 EVRM.

Artikel 8 EVRM is geen absoluut recht.

De uitzondering op de waarborg van de persoonlijke levenssfeer houdt in 'dat de inmenging door enig openbaar gezag in de privacyrechten moet voldoen aan de vereisten inzake noodzakelijkheid in een democratische samenleving en evenredigheid, en dat derhalve de inmenging specifieke, expliciete en legitieme doeleinden moeten dienen en moet plaatsvinden op adequate en relevante wijze, en niet buitensporig mag zijn in verhouding tot het doel van de inmenging.' (Richtlijn 2006/24/EG, overweging 25).

3.2.

Eerste onderdeel

Samenvatting van het middelonderdeel

Dit onderdeel richt zich tegen artikel 5 van de bestreden wet van 30 juli 2013 in haar geheel, waarbij artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, wordt vervangen. Minstens richt dit onderdeel zich tot de §§ 1 tot en met 5 van vermeld artikel 126.

De essentie van het onderdeel is dat de wetsbepalingen in strijd zijn met de vermelde artikels van de Grondwet al of niet in samenhang met de vermelde andere rechtsnormen, en inzonderheid dat ze in strijd zijn met artikel 10, 11 en 22 van de Grondwet, artikel 8 EVRM, artikel 7, 8, 11 en 52.1 van het Handvest en artikel 5 § 4 van het Verdrag EU.

Het recht op privacy, de eerbiediging van de persoonlijke levenssfeer en de bescherming van de persoonlijke data worden door vermeld artikel geschonden.

Dit onderdeel refereert naar het advies van de advocaat-generaal van 12 december in de samengevoegde zaken C-293/12 en C-594/12 voor het Europees Hof van Justitie.

3.2.1.

De richtlijn 2006/24/EG van 15 maart 2006 is op zich en in haar geheel strijdig met artikel 52, § 1 van het Handvest en is wat artikel 6 betreft strijdig met artikel 7 en artikel 52 § 1 van het Handvest. De richtlijn 2006/24/EG is strijdig met artikel 5 § 4 EU verdrag.

47.

Het hier bestreden artikel 5 van de wet van 30 juli 2013 is de omzetting in België van de richtlijn 2006/24/EG.

In de zaken C-293/12 (Ierland) en C-594/12 (Oostenrijk) van het Hof van Justitie van de Europese Unie, respectievelijk Digital Rights Ireland Ltd versus The Minister for Communications, Marine and Natural Ressources, The Minister for Justice, Equality and Law Reform, The Commisioner of the Garda Siochana Ireland and The Attorney General, en Kärtner Landesregierung, Michael Seitlinger en Christof Tscholl e.a. heeft de Advocaat Generaal op 12 december 2013 een advies uitgebracht waarin hij stelt dat de Richtlijn 2006/24/EG van 15 maart 2006 betreffende de bewaring van gegevens… in haar geheel onverenigbaar is met artikel 52 (1) van het Handvest en wat artikel 6 van de Richtlijn betreft dat deze onverenigbaar is met artikel 7 en 52 (1) van het Handvest.

Verzoekers onderzoeken de relevante passages van het advies. Het integrale advies wordt als stuk 6 gevoegd. De verwijzingen in de geciteerde passages zijn terug te vinden in dat stuk.

De onderlijning in de citaten van het advies zijn van verzoekers.

48.

Het advies onderzoekt de verhouding tussen de Richtlijn 2006/24/EG en de Richtlijn 95/46/EG en 2002/58/EG.

Het advies stelt duidelijk dat de Richtlijn 95/46/EG en 2002/58/EG in essentie bedoeld zijn om aan de burgers het vertrouwelijk karakter van elektronische communicatie te verzekeren:

> 1. „Functionele dualiteit" van richtlijn 2006/24 en de verhouding ervan tot richtlijn 95/46 en richtlijn 2002/58
>
> 31. Om te beginnen moet richtlijn 2006/24 in haar context worden geplaatst, waartoe ik kort zal ingaan op het wetgevingskader waarvan zij deel uitmaakt, dat hoofdzakelijk bestaat uit eerste richtlijn 95/46 en richtlijn 2002/58.
>
> 32. Richtlijn 95/46, die net als richtlijn 2006/24 is gebaseerd op artikel 114 VWEU, verplicht de lidstaten het recht op persoonlijke levenssfeer van natuurlijke personen in verband met de verwerking van hun persoonsgegevens te waarborgen(18), om het vrije verkeer van deze gegevens tussen lidstaten mogelijk te maken.(19) De richtlijn bevat daartoe onder meer regels inzake de voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens, de rechten van degenen wier gegevens worden verzameld en verwerkt, in het bijzonder het recht op informatie(20), het recht van

toegang(21), het recht van verzet(22) en het recht van beroep(23), en de waarborging van de vertrouwelijkheid en de beveiliging van de verwerking.

33. Op de beschermingsregeling die bij richtlijn 95/46 is ingesteld, bestaan uitzonderingen en beperkingen, omschreven in artikel 13 ervan. De omvang van de rechten en verplichtingen die hierin zijn bepaald met betrekking tot de kwaliteit van de gegevens (artikel 6, lid 1), de transparantie van de verwerking (artikelen 10 en 11, lid 1), de rechten van toegang voor personen wier gegevens worden verwerkt (artikel 12) en de openbaarheid van de verwerkingen (artikel 21), kan door wettelijke maatregelen worden beperkt indien dat noodzakelijk is voor onder meer de staatsveiligheid, defensie, de openbare veiligheid of het onderzoeken, opsporen en vervolgen van strafbare feiten.

34. Richtlijn 2002/58, die richtlijn 97/66/EG(24) heeft ingetrokken en vervangen, preciseert de regeling ter bescherming van persoonsgegevens van richtlijn 95/46 en vult(25) deze aan met specifieke regels voor de sector elektronische communicatie.(26) De richtlijn bevat met name regels die de lidstaten verplichten om, behoudens uitzonderingen(27), het vertrouwelijke karakter van niet alleen de communicatie, maar ook van de verkeersgegevens van de abonnees en de gebruikers van elektronische-communicatiediensten te beschermen.(28) Artikel 6 ervan verplicht aanbieders van communicatiediensten om de verkeersgegevens met betrekking tot hun abonnees en gebruikers die zij opslaan en verwerken, te wissen of anoniem te maken.

35. Van bijzonder belang voor het onderstaande betoog is artikel 15, lid 1, van richtlijn 2002/58, dat bepaalt dat de lidstaten wettelijke maatregelen kunnen(29) treffen ter beperking van de reikwijdte van de in de richtlijn bepaalde rechten en verplichtingen met betrekking tot onder meer het vertrouwelijke karakter van communicatie (artikel 5) en het wissen van verkeersgegevens (artikel 6) onder dezelfde voorwaarden als artikel 13, lid 1, van richtlijn 95/46, waarnaar het verwijst. Artikel 15, lid 1, benadrukt dat de lidstaten daartoe onder andere wettelijke maatregelen kunnen treffen om gegevens gedurende een beperkte periode te bewaren om een van de vermelde redenen, onder eerbiediging van de grondrechten.

49.

Het advies wijst er op dat de Richtlijn 2006/24/EG op de eerste plaats bedoeld is voor harmonisatie van de wetgevingen in de EU-landen in het kader van het goed functioneren van de interne markt.

Verder stelt het advies dat die Richtlijn een belangrijke wijziging aanbrengt met betrekking tot de rechtssituatie van data van elektronische communicatie door de verplichting tot bewaren ervan op te leggen met het oog op het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.

36. Met de bepaling dat de lidstaten voorzien in de verplichting om verkeers- en locatiegegevens te verzamelen en te bewaren, die valt onder de beperkingen van het recht op bescherming van persoonsgegevens die zijn bepaald in artikel 13, lid 1, van richtlijn

95/46 en artikel 15, lid 1, van richtlijn 2002/58, leidt richtlijn 2006/24 in werkelijkheid tot een diepgaande wijziging van de stand van het recht dat van toepassing is op gegevens in verband met elektronische communicatie en voortvloeit uit de richtlijnen 95/46 en 2002/58.(30)

37. Richtlijn 2006/24 wordt allereerst gekenmerkt door haar doelstelling van harmonisatie, in casu van de regelingen van de lidstaten met betrekking tot de bewaring van verkeers- en localisatiegegevens inzake elektronische communicatie. Gelet op het te harmoniseren onderwerp en de omstandigheden, brengt deze doelstelling tegelijkertijd mee dat lidstaten die niet over een dergelijke regeling beschikken, de verplichting wordt opgelegd om deze gegevens te verzamelen en te bewaren. Hieruit vloeit voort dat richtlijn 2006/24 een tweeledige functie heeft, waarmee absoluut rekening moet worden gehouden om de door de onderhavige prejudiciële vragen opgeworpen problematiek op juiste wijze te benaderen.

38. De eerste doelstelling van richtlijn 2006/24 is namelijk de onderlinge aanpassing van de nationale regelingen die aanbieders van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken(31) al verplichten de in de richtlijn aangegeven verkeers- en localisatiegegevens te bewaren, teneinde te waarborgen dat zij beschikbaar zijn „voor het onderzoeken, opsporen en vervolgen van zware criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten”(32). Hiermee harmoniseert richtlijn 2006/24 dus deels de regelingen die door bepaalde lidstaten zijn vastgesteld op basis van de optie in artikel 15, lid 1, van richtlijn 2002/58.(33)

39. Richtlijn 2006/24 voert derhalve een regeling in die afwijkt(34) van de beginselen van de richtlijnen 95/46 en 2002/58. Om precies te zijn, wijkt de richtlijn af van de afwijkende regels van artikel 15, lid 1, van richtlijn 2002/58 inzake de mogelijkheid voor de lidstaten om, op de in artikel 13, lid 1, van richtlijn 95/46 bepaalde gronden, de omvang van het recht op bescherming van persoonsgegevens, en meer in het algemeen het recht op eerbiediging van het privéleven, in het specifieke kader van het aanbod van elektronische communicatiediensten of van openbare communicatienetwerken, te beperken.

…

41. Zoals het Hof heeft opgemerkt in zijn arrest Ierland/Parlement en Raad, heeft richtlijn 2006/24 hoofdzakelijk betrekking op de activiteiten van aanbieders van elektronische communicatiediensten(35), aangezien de nationale regelingen worden geharmoniseerd door middel van bepalingen die in wezen zijn beperkt(36) tot het bewaren van gegevens, de te bewaren categorieën gegevens, de bewaringstermijn, de gegevensbescherming en de gegevensbeveiliging, alsook de opslag daarvan.(37)

…

46. Samenvattend wordt richtlijn 2006/24 gekenmerkt door haar functionele dualiteit. Enerzijds is het een heel klassieke richtlijn die streeft naar harmonisatie(42) van de nationale wettelijke bepalingen die verschillen(43) of dit in de toekomst kunnen gaan doen, en die is vastgesteld in het belang van de werking van de interne markt en hiertoe

nauwkeurig is afgestemd, zoals het Hof heeft aangegeven in het arrest Ierland/Parlement en Raad. Anderzijds is het echter tevens een richtlijn die, zelfs in haar harmoniserende functie, in voorkomend geval verplichtingen schept(44), in het bijzonder tot het bewaren van gegevens, en die verplichtingen betekenen, zoals ik hierna zal laten zien, klaarblijkelijke inmengingen in het genot van de grondrechten die door het Handvest aan de Europese burgers worden gewaarborgd, in het bijzonder het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens.

50.

Het advies stelt dat de Richtlijn 2006/24/EG onbetwistbaar een inmenging betekent in het fundamenteel recht op respect voor het privéleven zoals vastgelegd in artikel 7 Handvest en in artikel 8 Handvest, maar ook gevolgen heeft voor het zelfbeschikkingsrecht inzake informatieverwerving en de meningsvrijheid opgenomen in artikel 11 Handvest.

52. Allereerst kan er zeker niet aan worden voorbijgegaan dat het vage gevoel van gecontroleerd worden(45) dat de uitvoering van richtlijn 2006/24 kan veroorzaken, een bepalende invloed kan hebben op de uitoefening door Europese burgers van hun vrijheid op meningsuiting en van informatie, en dat dientengevolge tevens een inmenging in het door artikel 11 van het Handvest gewaarborgde recht moet worden vastgesteld.(46)

…

54. Richtlijn 2006/24 moet dus hoofdzakelijk worden getoetst op de verenigbaarheid met de artikelen 7 en 8 van het Handvest.

ii) Het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens in onderling verband

…

56. Richtlijn 2006/24 is een aanzienlijke aantasting van het recht op bescherming van persoonsgegevens, aangezien artikel 5 de lidstaten verplicht te zorgen voor de bewaring van gegevens die een persoon identificeren of kunnen identificeren(48), zowel aan de bron als bij de bestemming van een communicatie, alsmede zijn locatie in de ruimte en in de tijd, of dit nu geschiedt met behulp van zijn telefoonnummer voor de telefonie, zijn identificatienummer of enige andere hem betreffende informatie, zoals een IP-adres voor internetdiensten.

57. Artikel 2, lid 1, van richtlijn 2006/24 vermeldt overigens uitdrukkelijk dat de richtlijn onder meer van toepassing is op de gegevens die nodig zijn om de abonnees of geregistreerde gebruikers van elektronische communicatiediensten of openbare communicatienetwerken te identificeren. Deze gegevens vallen aldus onder de gegevens waarvan voor openbaarmaking de uitdrukkelijk toestemming nodig is van ieder individu, en daarmee onder iemands „zelfbeschikkingsrecht inzake zijn eigen informatie”(49).

58. Richtlijn 2006/24 komt op het eerste gezicht over als een inmenging in het recht op bescherming van persoonsgegevens, die duidelijk binnen het kader van de bepalingen van artikel 8, leden 2 en 3, van het Handvest valt. De richtlijn bepaalt namelijk dat zowel de richtlijnen 95/46 en 2002/58(50) als het Verdrag van tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van

Europa van 1981(51) integraal van toepassing zijn op de gegevens die overeenkomstig de richtlijn worden bewaard.

…

61. Aangezien de „privésfeer" de kern vormt van de „persoonlijke levenssfeer", kan niet worden uitgesloten dat een regeling die het recht op bescherming van persoonsgegevens beperkt en in overeenstemming is met artikel 8 van het Handvest, niettemin kan worden beschouwd als een onevenredige aantasting van artikel 7 van het Handvest.

62. Het recht op bescherming van persoonsgegevens berust zonder twijfel op het grondrecht op eerbiediging van het privéleven(52), zodat, zoals het Hof al heeft benadrukt(53), de artikelen 7 en 8 van het Handvest nauw met elkaar zijn verbonden(54), zelfs zodanig dat kan worden gezegd dat zij voorzien in een „recht op persoonlijke levenssfeer bij de verwerking van persoonsgegevens".(55)

…

65. Er zijn echter ook gegevens die op een bepaalde manier meer dan persoonlijk zijn. Dit zijn gegevens die kwalitatief bezien hoofdzakelijk verband houden met het privéleven, met de vertrouwelijkheid van de persoonlijke levenssfeer, met inbegrip van de intimiteit. In deze gevallen begint het probleem dat persoonsgegevens meebrengen, al in een eerdere fase. Het probleem dat zich dan voordoet, zijn nog niet de waarborgen in verband met de verwerking van de gegevens, maar ligt al daarvóór, in de gegevens op zich, dat wil zeggen het feit dat de omstandigheden van het privéleven van iemand zich hebben kunnen uitkristalliseren in de vorm van gegevens, die dientengevolge in informatiesystemen kunnen worden verwerkt.

…

67. Gezien het bovenstaande, waarin de grondrechten die gezamenlijk het koppel vormen bestaande uit het recht op eerbiediging van het privéleven (artikel 7 van het Handvest) en het recht op bescherming van persoonsgegevens (artikel 8 van het Handvest) juist zijn „gepositioneerd", moet de geldigheid van richtlijn 2006/24 hoofdzakelijk worden getoetst vanuit het oogpunt van de inmenging in het recht op eerbiediging van het privéleven.

51.

Het advies kwalificeert de wetgeving opgelegd door de Richtlijn als een inmenging met een 'particulier karakter'.

b) Een bijzonder duidelijke inmenging in het recht op eerbiediging van het privéleven

68. Om te beginnen lijdt het nauwelijks twijfel dat richtlijn 2006/24 op zichzelf een „inmenging" vormt in het recht op eerbiediging van het privéleven.(56) In de richtlijn zelf wordt dit aangegeven door de omschrijving ervan als „instrument betreffende de bewaring van gegevens" dat „overeenkomstig de vereisten van artikel 8 van het EVRM [...] een

noodzakelijke maatregel”(57) vormt, of overeenkomstig die van artikel 7 van het Handvest. Het Hof gebruikt deze term overigens in verband met deze richtlijn.(58)

69. Het Europees Hof voor de Rechten van de Mens heeft zijnerzijds meermalen geoordeeld dat het opslaan van gegevens inzake het privéleven van een individu door een openbare autoriteit een inmenging vormt in het door artikel 8, lid 1, EVRM gewaarborgde recht op de eerbiediging van zijn privéleven(59), waarbij het benadrukte dat het van weinig belang is welk gebruik ervan wordt gemaakt.(60)

70. In het onderhavige geval moet worden getracht deze inmenging te kwalificeren. Zoals ik hierna meer in detail zal aangeven, kan in zoverre worden gesteld dat richtlijn 2006/24 een *bijzonder duidelijke*(61) inmenging vormt in het recht op eerbiediging van het privéleven.

71. Richtlijn 2006/24 sluit weliswaar op even uitdrukkelijke als dringende wijze(62) de inhoud van de telefonische of elektronische communicatie, dus de gecommuniceerde informatie zelf, uit van de werkingssfeer ervan.

72. Dat neemt niet weg dat het verzamelen(63) en vooral het bewaren(64), in gigantische databases, van de talloze gegevens die zijn gegenereerd of verwerkt in het kader van het grootste deel van de gebruikelijke elektronische communicatie van de burgers van de Unie(65), een duidelijke inmenging in hun privéleven vormt, ook al worden daarmee enkel de voorwaarden geschapen om achteraf hun persoonlijke alsook beroepsmatige activiteiten te kunnen controleren. Het verzamelen van deze gegevens creëert de voorwaarden voor een toezicht dat, ook al wordt dit slechts met terugwerkende kracht uitgevoerd bij de exploitatie van de gegevens, niettemin, zolang de gegevens worden bewaard, het recht van de burgers van de Unie op vertrouwelijkheid van hun persoonlijke levenssfeer permanent bedreigt. Het opgewekte vage gevoel van gecontroleerd worden(66) leidt bijzonder acuut tot de vraag wat de bewaringstermijn van de gegevens is.

73. Dienaangaande moet ten eerste rekening worden gehouden met het feit dat de gevolgen van deze inmenging worden verveelvoudigd door de plaats die de elektronische communicatiemiddelen in de moderne samenleving hebben ingenomen, of het nu gaat om digitale mobiele netwerken dan wel om internet, en het massale en intensieve gebruik ervan door een zeer groot deel van de Europese burgers op alle terreinen van hun privé- of beroepsactiviteiten.(67)

74. De betrokken gegevens, zo wil ik nogmaals benadrukken, zijn geen persoonsgegevens in de klassieke zin des woords die verband houden met precieze informatie over de identiteit van personen, maar in feite “gekwalificeerde” persoonsgegevens, die, wanneer zij worden geëxploiteerd, een belangrijk deel van het gedrag van een persoon, dat strikt onder zijn privéleven valt, op getrouwe en uitputtende wijze in kaart kunnen brengen of zelfs een volledig en precies beeld kunnen schetsen van zijn privé-identiteit.

75. De intensiteit van deze inmenging wordt des te duidelijker door factoren die het risico vergroten dat de bewaarde gegevens, ondanks de verplichtingen die door richtlijn 2006/24 aan zowel de lidstaten zelf als de aanbieders van elektronische communicatiediensten worden opgelegd, worden gebruikt voor onrechtmatige doeleinden die potentieel inbreuk maken op het privéleven, of ruimer, voor frauduleuze of zelfs kwaadwillende doeleinden.

76. Deze gegevens worden namelijk niet bewaard door de autoriteiten zelf of zelfs maar onder hun directe toezicht, maar door de aanbieders van elektronische communicatiediensten(68), op wie het merendeel van de verplichtingen rust die als waarborg van de bescherming en de veiligheid van de gegevens moeten dienen.

…

78. Richtlijn 2006/24 bevat echter geen enkele bepaling die deze dienstenaanbieders verplicht de gegevens zelf te bewaren op het grondgebied van een lidstaat, dat onder de rechtsmacht van een lidstaat valt, hetgeen het risico dat zij in strijd met deze regeling toegankelijk of openbaar gemaakt worden, aanzienlijk vergroot.

79. Door deze „outsourcing" van de gegevensbewaring kunnen de bewaarde gegevens inderdaad uit de buurt worden gehouden van de autoriteiten van de lidstaten en dus worden onttrokken aan hun directe greep en aan alle controle(70), maar wordt tegelijkertijd het risico vergroot dat de gegevens worden geëxploiteerd op een wijze die niet in overeenstemming is met de eisen die voortvloeien uit het recht op eerbiediging van het privéleven.

80. Richtlijn 2006/24 vormt dus, zoals blijkt uit het voorgaande, een bijzonder duidelijke inmenging in het recht op eerbiediging van het privéleven. De geldigheid, en de evenredigheid ervan in het bijzonder, moet primair worden onderzocht in het licht van de eisen die voortvloeien uit dit grondrecht.

52.

Het advies stelt dat de Richtlijn niet proportioneel is in het kader van artikel 5, §4 Verdrag EU.

102. De duidelijke inmenging in recht op eerbiediging van het privéleven die de lidstaten, als gevolg van de constitutieve werking van richtlijn 2006/24 geacht worden op te nemen in hun eigen rechtsorde, lijkt aldus buiten verhouding te staan tot enkel de noodzaak om de werking van de interne markt te waarborgen, ook al worden dit verzamelen en bewaren overigens als geschikte en zelfs noodzakelijke middelen beschouwd ter bereiking van de uiteindelijke doelstelling van de richtlijn, namelijk ervoor zorgen dat de gegevens beschikbaar zijn voor het opsporen en vervolgen van zware criminaliteit. Samenvattend zou richtlijn 2006/24 de evenredigheidstoets niet doorstaan op basis van de redenen die de keuze van haar rechtsgrondslag rechtvaardigden. Paradoxaal genoeg zouden de redenen die haar sauveerden vanuit het oogpunt van de rechtsgrondslag, de redenen zijn waarom zij geen stand houdt in het licht van de evenredigheid.

53.

Het advies stelt dat de Richtlijn in strijd is met artikel 52.1 van het Handvest en meer specifiek inzake de kwaliteit van de wet en de evenredigheid op zich.

> 107. Meer in het algemeen is de inmenging in het recht op eerbiediging van het privéleven, die wordt gevormd door richtlijn 2006/24, enkel aanvaardbaar voor zover deze voldoet aan de voorwaarden van artikel 52, lid 1, van het Handvest, dus indien zij „bij wet" is gesteld en meer bepaald voldoet aan de vereisten betreffende de kwaliteit van de wet, de wezenlijke inhoud van dat recht eerbiedigt en evenredig is, dat wil zeggen noodzakelijk is voor en daadwerkelijk voldoet aan door de Unie erkende doelstellingen van algemeen belang, of noodzakelijk is ten behoeve van de bescherming van de rechten en vrijheden van anderen.

54.

Strijdigheid inzake de kwaliteit van de wet.

> 1. Kwaliteit van de wet
>
> …
>
> 111. In een meer dan formele opvatting van het vereiste dat iedere beperking bij wet moet zijn bepaald, is het de vraag of de beperkingen die richtlijn 2006/24 aan de uitoefening van de grondrechten stelt, wel gepaard gaan met voldoende tot in detail bepaalde waarborgen die bij dergelijke beperkingen moeten worden voorzien.
>
> …
>
> 113. De moeilijkheid waarvoor richtlijn 2006/24 ons plaatst – ik herhaal het nog maar eens – is dat het een richtlijn betreft die enkel voorziet in een verplichting voor aanbieders van elektronische communicatiediensten om de verkeers- en localisatiegegevens van de elektronische communicatie te verzamelen en te bewaren, maar niet de waarborgen regelt die de toegang tot deze bewaarde gegevens en de exploitatie ervan moeten beheersen. Richtlijn 2006/24 laat dit punt, zoals wij hebben gezien, in algemene zin over aan de lidstaten.(89)
>
> 114. Zo geformuleerd, komt vraag er dus op neer of aan het vereiste dat iedere beperking van de grondrechten „bij wet moet worden gesteld", wordt voldaan door een dergelijke algemene verwijzing, ook al gaat deze gepaard met uitdrukkelijk vermelding van de rechten gewaarborgd in de richtlijnen 95/46 en 2002/58.
>
> …
>
> 117. In het tweede geval daarentegen, wanneer de beperking van de grondrechten voortvloeit uit wetgeving van de Unie zelf en derhalve aan de Unie is toe te schrijven, krijgt de wetgever van de Unie een heel ander deel in de verantwoordelijkheid. In het geval van een richtlijn is het duidelijk dat het aan de lidstaten is de waarborgen nader uit te werken die een kader moeten vormen voor een beperking van de grondrechten in een geval als het onderhavige. Niettemin lijkt er voor de wetgever van de Unie ook een leidende rol weggelegd bij de eigenlijke invulling van deze waarborgen. Vanuit dit

gezichtspunt moet worden onderzocht of het vereiste betreffende de kwaliteit van de wet is geëerbiedigd.

118. Met andere woorden, de overgang van een facultatieve regeling zoals kon worden vastgesteld op basis van artikel 15 van richtlijn 2002/58, naar een op termijn prescriptieve regeling zoals die is ingevoerd bij richtlijn 2006/24, had gepaard moeten gaan met een gelijktijdige ontwikkeling op het gebied van de waarborgen en had dus voor de wetgever van de Unie principieel aanleiding moeten zijn te specificeren welke beginselen gelden voor het kader waarin de toegang tot de gegevens en de exploitatie ervan op zeer uitgebreide schaal aan de lidstaten werd gedelegeerd.

119. Dienaangaande moet namelijk allereerst worden opgemerkt dat zowel richtlijn 95/46 als richtlijn 2002/58 benadrukt dat de maatregelen ter beperking van de gewaarborgde rechten die de lidstaten mogen vaststellen, wettelijk van aard moeten zijn.(90) Richtlijn 2006/24 noemt deze formele eis echter slechts zijdelings(91) en verlaagt zo het niveau van de waarborgen die zijn ingesteld in de richtlijnen waarvan zij afwijkt.(92)

120. De wetgever van de Unie kan namelijk, wanneer hij een handeling vaststelt die verplichtingen oplegt die een duidelijke inmenging vormen in de grondrechten van de burgers van de Unie, het niet volledig aan de lidstaten overlaten om de waarborgen te regelen die deze inmenging kunnen rechtvaardigen. Hij kan er niet mee volstaan om het bepalen en vaststellen van die waarborgen over te laten aan de wetgevende en/of bevoegde bestuurlijke autoriteiten van de lidstaten die, in voorkomend geval, nationale maatregelen ter uitvoering van een dergelijke handeling moeten vaststellen, noch ook zich geheel te verlaten op het toezicht op de concrete toepassing ervan door de gerechtelijke autoriteiten. Op het gevaar af van uitholling van artikel 51, lid 1, van het Handvest, behoort hij zijn deel van de verantwoordelijkheid volledig op zich nemen door ten minste de beginselen te definiëren die leidend moeten zijn bij de bepaling, de vaststelling, de toepassing en het toezicht op de eerbiediging van deze waarborgen.

121. Er is bij herhaling gesteld dat richtlijn 2006/24, zoals staat vermeld in artikel 4 ervan(93), de *toegang*(94) tot de verzamelde en bewaarde gegevens, noch de exploitatie ervan regelt. Zij kon dat overigens ook niet, gelet op de verdeling van de bevoegdheden tussen de lidstaten en de Unie.(95) De vraag is nu echter juist of de Unie een maatregel als de betrokken verplichting om gegevens te verzamelen en duurzaam te bewaren *kan*(96) vaststellen zonder deze maatregel tegelijkertijd te omringen met waarborgen ten aanzien van de voorwaarden die moeten gelden voor de toegang en de exploitatie van die gegevens, ten minste in de vorm van beginselen. Het is nu juist deze regeling van de voorwaarden voor toegang tot en exploitatie van de verzamelde en bewaarde gegeven waardoor kan worden getoetst wat deze inmenging concreet betekent en of deze inmenging dus constitutioneel gezien al dan niet aanvaardbaar kan zijn.

…

123. Ook al was de rechtsgrondslag van richtlijn 2006/24 die inzake waarborging van de goede werking van de interne markt en konden de voorwaarden voor toegang tot en de exploitatie van de gegevens niet alle in de bepalingen ervan worden opgenomen, vereist de constitutieve werking van de verplichting tot verzamelen en bewaren die zij bevat, dat de richtlijn werd voorzien van een reeks principiële waarborgen als noodzakelijk en

onmisbaar complement. Hiertoe kan niet worden volstaan met de algemene verwijzing naar de lidstaten, en ook de beschermingsregeling van richtlijn 95/46(97) of van kaderbesluit 2008/977(98) kan hier, bij gebreke van toepasselijkheid, geen oplossing bieden.

…

125. Ik ben derhalve van mening dat het aan de wetgever van de Unie was de fundamentele beginselen aan te geven die in acht moesten worden genomen bij het bepalen van de minimumwaarborgen voor de toegang tot de verzamelde en bewaarde gegevens en de exploitatie ervan, Zonder uitputtend te zijn zou ik in dit verband willen noemen.

127. Hij had de regelgeving van de lidstaten voor de toestemming voor toegang tot de verzamelde en bewaarde gegevens moeten oriënteren door de toegang te beperken tot enkel de gerechtelijke autoriteiten(100) dan wel ten minste tot onafhankelijke autoriteiten, of anders ieder verzoek tot toegang te onderwerpen aan het toezicht van de gerechtelijke autoriteiten of onafhankelijke autoriteiten en verplicht te stellen dat ieder verzoek tot toegang afzonderlijk wordt onderzocht, teneinde de meegedeelde gegevens tot het strikt noodzakelijke te beperken.

…

130. Dat de verschillende, hierboven niet uitputtend opgesomde waarborgen noodzakelijk zijn, wordt bevestigt door de omstandigheid dat de wetgever van de Unie zelf, na de vaststelling van richtlijn 2006/24, kaderbesluit 2008/977 heeft vastgesteld, dat de bescherming garandeert van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, en nu juist in dit soort waarborgen voorziet, al is het enkel in het kader van verzending van gegevens tussen lidstaten. Kaderbesluit 2008/977 sluit namelijk de gegevens die niet onder de uitwisseling tussen lidstaten vallen, uit van de werkingssfeer ervan, zoals met name blijkt uit punt 9 van de considerans van kaderbesluit 2008/977.(101)

131. Concluderend meen ik dat richtlijn 2006/24 in haar geheel onverenigbaar is met artikel 52, lid 1, van het Handvest, aangezien de beperkingen die zij aan de uitoefening van de grondrechten stelt door de opgelegde verplichting tot het bewaren van gegevens, niet gepaard gaan met de onmisbare beginselen die hebben te gelden voor de waarborgen waarmee de toegang tot deze gegevens en de exploitatie ervan behoren te zijn omkleed.

55.

Het advies stelt ook dat de Richtlijn het begrip ‘criminele activiteiten’ nauwkeuriger had moeten omschrijven.

126. Gelet op de intensiteit van de inmenging behoorde de wetgever van de Europese Unie de criminele activiteiten die de toegang van de bevoegde nationale autoriteiten tot de verzamelde en bewaarde gegevens rechtvaardigen, nauwkeuriger te omschrijven dan met de uitdrukking „zware criminaliteit”(99).

56.

Strijdigheid van de richtlijn met het evenredigheidsbeginsel

2. Evenredigheid in de zin van artikel 52, lid 1, van het Handvest

133. Artikel 52, lid 1, van het Handvest vereist niet alleen dat iedere beperking van de uitoefening van de grondrechten „bij wet wordt gesteld", maar ook dat deze beperking plaatsvindt onder strikte eerbiediging van het evenredigheidsbeginsel. Dit evenredigheidsvereiste krijgt, zoals ik reeds heb benadrukt, in de context van het Handvest een bijzondere kracht, die het niet heeft in het kader van artikel 5, lid 4, VEU. Hier gaat het namelijk niet om evenredigheid als algemeen beginsel voor het optreden van de Unie, maar meer specifiek om evenredigheid als constitutieve voorwaarde voor enige beperking van grondrechten.

134. Vanuit dit gezichtspunt kan het nastreven door de instellingen van de Unie van de in richtlijn 2006/24 aangekondigde doelstelling, namelijk ervoor zorgen dat de bewaarde gegevens beschikbaar zijn voor de vervolging van zware criminaliteit, enkel geoorloofd zijn indien dit in overeenstemming is met, in het bijzonder, het recht op eerbiediging van het privéleven.(103)

135. Niettemin ben ik van mening dat, gelet op de hierboven onderzochte vereisten volgens welke de „wet", ten minste in de vorm van beginselen, voldoende waarborgen dient te bevatten met betrekking tot de toegang tot de gegevens die worden verzameld en bewaard door de aanbieders van elektronische communicatiediensten en de exploitatie ervan, de evenredigheid van de door richtlijn 2006/24 opgelegde bewaringsverplichting als zodanig, op een enkele uitzondering na, niet langer noopt tot een bijzonder diepgaand onderzoek dat verder gaat dan hetgeen hier volgt.

136. Richtlijn 2006/24 streeft namelijk een geheel legitiem doel na, het garanderen dat verzamelde en bewaarde gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van zware criminaliteit, en kan, gelet op de beperkte toetsing dat het Hof in dat opzicht kan uitvoeren, worden beschouwd als passend en zelfs, onder voorbehoud van de waarborgen die hiermee gepaard zouden moeten gaan, als noodzakelijk om deze uiteindelijke doelstelling te bereiken.(104) Deze waarborgen in het bijzonder kunnen de, zeker zeer lange, lijst van categorieën gegevens die moeten worden bewaard, genoemd in artikel 5, van richtlijn 2006/24, rechtvaardigen.

…

138. Vanuit het oogpunt van de noodzakelijkheid van de maatregel wil ik evenwel met nadruk wijzen op het belang van artikel 14 van richtlijn 2006/24, dat de Commissie verplicht *een*(105) evaluatieverslag(106) uit te brengen over de toepassing ervan, op basis van met name statistische informatie die de lidstaten moeten opstellen overeenkomstig artikel 10, en op deze basis wijzigingen voor te stellen die in voorkomend geval noodzakelijk zijn, in het bijzonder wat betreft de lijst van de categorieën gegevens die moeten worden verzameld en bewaard en de bewaringstermijn.

139. In die zin, en ook aangezien richtlijn 2006/24 geen enkele bepaling bevat die in de expiratie ervan voorziet („sunset clause), is het de plicht van de wetgever van de Unie om de omstandigheden die de duidelijke beperking van de uitoefening van het recht op

eerbiediging van het privéleven in de richtlijn rechtvaardigen, regelmatig opnieuw te evalueren, zodat hij kan nagaan of deze omstandigheden nog steeds bestaan en dientengevolge deze beperking kan bijstellen of zelfs intrekken.

140. Terugkomend op de zojuist bedoelde uitzondering, deze heeft betrekking op de evenredigheid van artikel 6 van richtlijn 2006/24, dat de bewaringstermijn van de verzamelde gegevens definieert.

141. Artikel 6 van richtlijn 2006/24 regelt een van de fundamentele aspecten van de door de richtlijn geharmoniseerde of, in voorkomend geval, ingevoerde bewaring van gegevens, namelijk de in tijd beperkte omvang ervan. Alle bewaarde gegevens moeten namelijk in beginsel na verloop van tijd worden vernietigd, en dit kan ook niet anders. Anders dan de regel van richtlijn 2002/58, waarvan artikel 6, lid 1, bepaalt dat de verwerkte en opgeslagen verkeersgegevens moeten worden gewist of anoniem gemaakt zodra zij niet langer nodig zijn voor de transmissie van communicatie(107), is de verplichting te zorgen voor vernietiging van deze gegevens niet vrijwel onmiddellijk toepasselijk, maar pas na verloop van enige tijd. De lidstaten moeten garanderen dat de verzamelde gegevens worden bewaard gedurende een termijn die in geen geval korter mag zijn dan zes maanden en, onder voorbehoud van de afwijking in artikel 12 van richtlijn 2006/24, niet langer mag zijn dan twee jaar en concreet moet worden vastgesteld door de nationale wetgevers.

142. Met deze bepaling krijgt de bewaring van gegevens („data retention") waarmee wij ons bezighouden, een dimensie van chronologische continuïteit, die op beslissende wijze bijdraagt aan het karakteriseren van de inmenging in het recht op eerbiediging van het privéleven die richtlijn 2006/24 meebrengt, met name in vergelijking met de inmenging die zou ontstaan door het bewaren van gegevens achteraf („data preservation"), de zogenoemde „quick freeze".(108) De idee dat de betrokken gegevens gedurende een bepaalde tijd verzameld moeten blijven, is een van de hoofdaspecten van een maatregel die tot doel heeft het reactievermogen van de overheid groter ten aanzien van bepaalde ernstige vormen van criminaliteit te verbeteren. De vraag is echter of de bewoordingen waarin artikel 6 van richtlijn 2006/24 een minimum van zes maanden en een maximum van twee jaar oplegt, op passende wijze voldoen aan de vereisten van het evenredigheidsbeginsel.

143. In zoverre moet nog, zodra als vaststaand kan worden beschouwd dat de maatregel op zich legitiem en passend is, worden getoetst of de maatregel noodzakelijk is, en moet concreet worden nagegaan of de nagestreefde doelstelling niet zou kunnen worden bereikt met een maatregel die het genot van de betrokken grondrechten minder verstoort. Vanuit dit oogpunt wil ik graag benadrukken dat men niet eenvoudig kan stellen dat de lidstaten als enige verantwoordelijk zijn voor het eventueel vaststellen van een bewaringstermijn van twee jaar. Zodra richtlijn 2006/24, in haar harmoniserende functie, de bovengrens voor het bewaren van gegevens op twee jaar stelt, moet deze bepaling zelf op evenredigheid worden getoetst. Op dit punt hoeft er nauwelijks aan te worden herinnerd dat het niet de vraag is of, vanuit het oogpunt van de bestrijding van zware criminaliteit, een langere termijn voor bewaring en terbeschikkingstelling de voorkeur verdient boven

een kortere termijn, maar of er, in het kader van een onderzoek naar de evenredigheid ervan, een specifieke noodzaak voor bestaat.

144. Dienaangaande wil ik in de eerste plaats opmerken dat de opeenstapeling van gegevens op onbepaalde plaatsen in de cyberspace zoals hier in geding, die altijd nog concrete en bepaalde personen betreffen, ongeacht de duur ervan als een anomalie lijkt te worden gezien. In beginsel zou een dergelijke „retentie" van gegevens inzake het privéleven, ook al bleef het hiertoe beperkt, nooit mogen bestaan, en waar dat indien wel zo is, zouden daarvoor andere dwingende redenen van het maatschappelijk leven moeten bestaan. Een dergelijke situatie moet uitzonderlijk blijven en zou in die zin niet langer mogen duren dan absoluut noodzakelijk is.

145. De bewaringstermijn die als aanvaardbaar kan worden beschouwd in het licht van het evenredigheidsbeginsel, kan niet worden bepaald zonder dat de wetgever een zekere beoordelingsvrijheid wordt toegekend. Dit brengt echter niet mee dat op dit punt iedere toetsing van de evenredigheid – ook al is die moeilijk – is uitgesloten.

146. Dienaangaande lijkt het mij dienstig eraan te herinneren dat de mens zijn leven leidt gedurende een periode die per definitie beperkt is, waarin zowel het verleden, zijn eigen geschiedenis en uiteindelijk zijn herinnering alsook het heden, datgene wat min of meer onmiddellijk wordt beleefd, het bewustzijn van hetgeen hij beleeft, samensmelten.(109) Het verleden wordt van het heden gescheiden door een lijn, ook al is deze moeilijk te definiëren en verschilt deze per persoon. Wat moeilijk te bestrijden lijkt, is de mogelijkheid onderscheid te maken tussen de perceptie van het heden en de perceptie van het verleden. In elk van deze percepties kan het bewustzijn van het eigen leven, in het bijzonder het „privéleven", als „geregistreerd" leven een rol spelen. En het maakt verschil of dit „geregistreerde leven" het leven is dat men beschouwt als het huidige leven, dan wel datgene dat men beleeft als zijn eigen geschiedenis.

147. Ik ben van mening dat deze overwegingen kunnen worden geprojecteerd op de analyse van de evenredigheid van artikel 6 van richtlijn 2006/24. Wanneer het beginsel dat al deze persoonlijke documentatie gedurende een bepaalde tijd wordt bewaard als legitiem wordt beschouwd, resteert de vraag of het onvermijdelijk is, dat wil zeggen noodzakelijk, om dit op te leggen aan particulieren voor een termijn die zich niet enkel uitstrekt over „de tijd in het heden", maar ook over „de tijd in het verleden".

148. In die zin, en hoewel ik mij volledig bewust ben van de subjectiviteit hiervan, kan worden gesteld dat een bewaringstermijn voor persoonsgegevens „gemeten in maanden" goed moet worden onderscheiden van een termijn „gemeten in jaren". De eerste termijn zou overeenstemmen met een tijdsbestek dat is gesitueerd in het leven gezien als het heden, de tweede met een tijdsbestek dat is gesitueerd in het leven gezien als herinnering. De inmenging in het recht op eerbiediging van het privéleven is vanuit dit gezichtspunt telkens anders, en de noodzaak van elk van deze inmengingen moet kunnen worden aangetoond.

149. Ofschoon voldoende lijkt te zijn aangetoond dat de inmenging in de dimensie van de tegenwoordige tijd noodzakelijk is, heb ik geen enkele rechtvaardiging gevonden voor een

inmenging die zich moet uitstrekken tot de tijd in het verleden. Directer gezegd, en zonder te ontkennen dat er criminele activiteiten bestaan die lang van tevoren worden voorbereid, heb ik in de verschillende standpunten ter verdediging van de evenredigheid van artikel 6 van richtlijn 2006/24, nergens een rechtvaardiging gevonden waarom de bewaringsduur van de gegevens die door de lidstaten moet worden vastgesteld niet korter dan maximaal een jaar zou mogen bedragen. Anders gezegd, en met alle voorzichtigheid die deze dimensie van de evenredigheidstoetsing altijd vereist, heeft geen enkel argument mij kunnen overtuigen van de noodzaak om de bewaring van de gegevens langer te laten duren dan een jaar.

150. Tot slot moet tevens worden benadrukt dat richtlijn 2006/24 zelf een aanvullend argument biedt met het systeem van verlenging van de maximale bewaringstermijn voor gegevens dat zij bevat. Artikel 12 van deze richtlijn biedt namelijk de lidstaten die worden geconfronteerd met specifieke omstandigheden, waarop hier niet nader wordt ingegaan, de mogelijkheid om de maximale bewaringstermijn van artikel 6 ervan te verlengen. Een dergelijke verlenging is echter slechts voor een beperkte periode mogelijk, moet worden gemotiveerd en ter kennis worden gebracht van de Commissie, die beschikt over een termijn van zes maanden om uitspraak te doen over de voorgenomen maatregelen, dat wil zeggen om na te gaan of deze neerkomen op willekeurige discriminatie of een verkapte vorm van handelsbeperking en of zij een belemmering vormen voor de werking van de interne markt.

151. Ook al kan de Commissie overeenkomstig artikel 12, lid 2, van richtlijn 2006/24 deze maatregel enkel om een beperkt aantal redenen verwerpen, sterkt het bestaan van dit verlengingssysteem mij in mijn idee dat de in artikel 6 van deze richtlijn bepaalde maximale bewaringstermijn van de gegevens, die bij gebreke van specifieke omstandigheden tot twee jaar kan bedragen, niet noodzakelijk is en moet worden beschouwd als onverenigbaar met de vereisten die voortvloeien uit de artikelen 7 en 52, lid 1, van het Handvest.

152. Hieruit volgt dat artikel 6 van richtlijn 2006/24 onverenigbaar is met de artikelen 7 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in zover dit de lidstaten verplicht ervoor te zorgen dat de in artikel 5 ervan bedoelde gegevens worden bewaard gedurende een termijn die tot twee jaar kan oplopen.

3.2.2.

Schendingen afgeleid uit het advies van de advocaat-generaal.

3.2.2.1.

57.

Het advies stelt dat de Richtlijn niet evenredig is met de vooropgestelde noodzaak om de interne markt te regelen (beschouwing 102) en bijgevolg in strijd is met artikel 5 § 4 van het Verdrag EU.

Artikel 5 §4 Verdrag EU:
"Krachtens het evenredigheidsbeginsel gaan de inhoud en de vorm van het optreden van de Unie niet verder dan wat nodig is om de doelstellingen van de Verdragen te verwezenlijken. De instellingen van de Unie passen het evenredigheidsbeginsel toe overeenkomstig het protocol betreffende de toepassing van de beginselen van subsidiariteit en evenredigheid."

De omzetting in Belgische wet van de Richtlijn is op zich bijgevolg ook in strijd met vermeld artikel van het Verdrag EU.

Artikel 5 van de wet van 30 juli 2013 is, inzonderheid door de vervanging van artikel 126 § 1, 3 en 5 van de wet van 13 juni 2005 betreffende de elektronische communicatie de invoering in België van de verplichting van de Richtlijn tot regeling van de interne markt.

Zoals hoger vermeld kan het Grondwettelijk Hof die Belgische wetsbepaling toetsen aan de norm van het Verdrag EU, op zich door een verdragsconforme interpretatie van de voorgelegde wet, minstens door het relateren van die bepaling van het Verdrag EU aan artikel 10, 11 en 22 Grondwet.

Verzoekers stellen, en volgen hierbij het advies van de advocaat-generaal, dat vermelde wetsbepalingen van artikel 5 van de wet van 30 juli 2013 strijdig zijn met artikel 5 & 4 Verdrag EU.

3.2.2.2.

58.

Met betrekking tot de mensenrechten stelt het advies dat de Richtlijn 2006/24/EG zelf, die de basis vormt voor de hier bestreden wetsbepaling, verworpen moet worden daar zij in haar geheel strijdig is met artikel 52(1) van het Handvest (beschouwing 131) en wat haar artikel 6 betreft strijdig met artikel 7 én 52 (1) van het Handvest (beschouwing 152).

Dit betekent dat de juridische basis zelf waarop het hier bestreden artikel 5 van de wet van 30 juli 2013 steunt strijdig is met vermelde bepalingen van het Handvest (en met de overeenstemmende artikels 8 EVRM en 22 Grondwet). Het logische gevolg is dat ook het hier bestreden artikel 5 van de wet van 30 juli 2013 dat precies de omzetting is in de Belgische rechtsorde van vermelde Richtlijn als in strijd met vermelde wetsbepalingen dient vernietigd te worden.

Artikel 52 (1) van het Handvest stelt:
"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 in achtneming 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."

Het advies is met betrekking tot de schending van artikel 52 (1) Handvest heel precies en duidelijk (zie beschouwingen 117-123).

> De EU-wetgever diende in het kader van de kwaliteit van de wetgeving zelf garanties in de Richtlijn in te bouwen en op een principiële manier in het kader van de ruime delegatie van bevoegdheden aan de Staten inzake de toegang tot en de exploitatie van data die garanties onder vorm van principes te specifiëren. De EU-wetgever mocht, wanneer hij aan de Staten een akte oplegt die constitutieve verplichtingen inhoudt of een constitutief effect heeft (verzamelen en bewaren van data) met betrekking tot een gekarakteriseerde inmenging in de fundamentele rechten van de burgers van de Unie, niet volledig de zorg overlaten aan de lidstaten zelf om garanties in te bouwen die van aard zijn de inmenging te rechtvaardigen. Dit niet doen is artikel 52 (1) van zijn inhoud ontdoen. Zijn verantwoordelijkheid met betrekking tot de invulling van dit artikel opnemen houdt in dat de EU-wetgever ten minste de principes definieert die moeten gerespecteerd worden bij de definitie, de opbouw, de toepassing en de controle op het respect van de garanties. Het constitutief karakter van de Richtlijn impliceert dat zij vergezeld moet gaan van een reeks van principiële garanties als een noodzakelijk en onmisbaar onderdeel bij de Richtlijn zelf. Dit overlaten aan de Staten zelf voldoet niet en ook het beschermingsregime ingesteld door de Richtlijn 95/46 en het kaderbesluit 2008/977 volstaat niet om hieraan te verhelpen.

Zoals hoger gesteld kan het Grondwettelijk Hof zelf direct de Belgische wet toetsen aan de vermelde supranationale bepaling, minstens door artikel 7 en 52 (1) Handvest en artikel 8 EVRM te relateren aan artikel 10, 11 en 22 van de Grondwet.

Deze nietigheid betreft het ganse artikel 5 van de wet van 30 juli 2013, daar dit artikel door de invoering van het nieuwe artikel 126 in de wet van 13 juni 2005 een volledig mechanisme van dataretentie invoert.

3.2.2.3.

59.

Het advies stelt dat de Richtlijn, rekening houdend met de intensiteit van de inmenging, een duidelijke omschrijving had moeten geven van de criminele activiteiten die de toegang van de bevoegde nationale overheden tot de verzamelde en bewaarde gegevens zouden rechtvaardigen. Het moet gaan om een grotere graad van precisering dan enkel het begrip ‘zware inbreuken’. (beschouwing 126).

Zoals hoger gesteld kan het Grondwettelijk Hof zelf direct de Belgische wet toetsen aan de vermelde supranationale bepaling, minstens door artikel 7 en 52 (1) Handvest en artikel 8 EVRM te relateren aan artikel 10, 11 en 22 van de Grondwet.

Het door artikel 5 van de wet van 30 juli 2013 ingevoerde artikel 126 § 2, a. bepaalt dat de gegevens bewaard worden met het oog op ‘de opsporing, het onderzoek en de vervolging van strafbare feiten zoals bedoeld in de artikelen 46bis en 88bis van het Wetboek van strafvordering.

Het begrip ‘strafbare feiten’ schendt de legaliteitsverplichting zoals geformuleerd in artikel 52 (1) Handvest en bijgevolg dient artikel 126 § 2, a vernietigd te worden.

3.2.2.4.

60.

Het advies stelt dat de Richtlijn wat betreft de duur van bewaring van de gegevens in strijd is met artikel 7 én 52 (1) van het Handvest, in de mate dat ze toelaat data te bewaren voor een duurtijd die twee jaar kan bedragen. Een duurtijd van twee jaar buiten het kader van buitengewone omstandigheden is niet verenigbaar met vermelde artikels. Het advies stelt dat een duurtijd in maanden en niet in jaren had moeten vooropgesteld worden, en dat het geen enkele rechtvaardiging vindt voor een inmenging die zich uitstrekt in de ‘historische tijd’ of ‘langer dan één jaar’. (beschouwingen 147-152). Een vork van zes maanden tot twee jaar voldoet niet aan de evenredigheidsverplichting (beschouwing 142-143). Het advies stelt dat het artikel 6 van de Richtlijn zelf bijgevolg in strijd is met vermelde artikels van het Handvest.

Zoals hoger gesteld kan het Grondwettelijk Hof zelf direct de Belgische wet toetsen aan de vermelde supranationale bepaling, minstens door artikel 7 en 52 (1) Handvest en artikel 8 EVRM te relateren aan artikel 10, 11 en 22 van de Grondwet.

Het door artikel 5 van de wet van 30 juli 2013 ingevoerde artikel 126 § 3 stelt een bewaringstermijn voorop van twaalf maanden voor de verkeers- en locatiegegevens en een termijn vanaf de inschrijving tot twaalf maanden na de laatst geregistreerde communicatie voor de identificatiegegevens.

Het door artikel 5 van de wet van 30 juli 2013 ingevoerde artikel 126 § 4 opent de mogelijkheid om de bewaringstermijn tot 18 maanden te verlengen, en zelfs langer dan 24 maanden in de omstandigheden van artikel 4 § 1 van de wet van 13 juni 2005 op de elektronische communicatie. Deze verlenging tot 18 maanden vereist geen tussenkomst van het parlement maar kan bij Koninklijk Besluit. De kwaliteit van de wet wordt geschonden door deze termijnverlenging uit handen van het parlement te halen en aan een KB over te laten.

Het door artikel 5 van de wet van 30 juli 2013 ingevoerde artikel 126 § 7 opent de mogelijkheid om na een evaluatie de bewaringstermijn aan te passen, wat inhoudt dat hij boven de 18 maanden kan gaan, welke nu als grens in de wet is opgelegd.

Zoals in het advies gesteld schenden deze termijnen zowel het wettigheidsbeginsel als het proportionaliteitsbeginsel.

De artikels 126 § 3, 4 en 7 dienen vernietigd te worden.

3.2.

Tweede onderdeel

Samenvatting van het middelonderdeel

Dit onderdeel richt zich tegen artikel 5 van de bestreden wet van 30 juli 2013 in haar geheel, waarbij artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, wordt vervangen. Minstens richt dit onderdeel zich tot de §§ 1 tot en met 5 van vermeld artikel 126.

De essentie van het onderdeel is dat de wetsbepalingen in strijd zijn met de vermelde artikels van de Grondwet al of niet in samenhang met de vermelde andere rechtsnormen, en inzonderheid dat ze in strijd zijn met artikel 10, 11, 19, 22 en 25 van de Grondwet, artikel 8 EVRM, artikel 7, 8 en 52.1 van het Handvest.

Het recht op privacy, de eerbiediging van de persoonlijke levenssfeer en de bescherming van de persoonlijke data worden door vermeld artikel geschonden.

Schending van het wettigheidsbeginsel, het evenredigheidsbeginsel en het subsidiariteitsbeginsel.

3.2.1.

A. Aard en omvang van de bewaarde gegevens schenden de privacy; er is niet aangetoond dat dergelijke inmenging in het privéleven beantwoordt aan een dwingende maatschappelijke behoefte. Noodzakelijkheidstoets en evenredigheidstoets.

61.

A.1.Verzoekers verwijzen naar het arrest van 9 november 2010, C-92/09 & C-93/9, inzake *Volker und Markus Schecke & Hartmut Eifert t. Land Hessen,* van het Europees Hof van Justitie met betrekking tot de noodzakelijkheidstoets (en evenredigheidstoets) inzake de inmenging in het recht op privacy:

> 74. Volgens vaste rechtspraak vereist het evenredigheidscriterium, dat deel uitmaakt van de algemene rechtsbeginselen van de Unie, dat de middelen waarmee een handeling van de Unie de nagestreefde doelstelling beoogt te bereiken, passend zijn en niet verder gaan dan daarvoor noodzakelijk is (arrest van 8 juni 2010, Vodafone e.a., C-58/08).
>
> 86. Uit het voorgaande blijkt dat de instellingen geen evenwichtige afweging lijken te hebben gemaakt tussen, enerzijds, de doelstellingen van artikel 44 bis van verordening nr. 1290/2005 en van verordening nr. 259/2008 en, anderzijds, de door de artikelen 7 en 8 van het Handvest aan natuurlijke personen toegekende rechten. Gelet op het feit dat de uitzonderingen op en beperkingen van de bescherming van persoonsgegevens binnen de grenzen van het strikt noodzakelijke moeten blijven (arrest Satakunnan Markkinapörssi en Satamedia, reeds aangehaald, punt 56) en dat maatregelen denkbaar zijn die voor natuurlijke personen een minder ingrijpende aantasting van voormeld fundamenteel recht meebrengen en tegelijkertijd doeltreffend bijdragen tot de verwezenlijking van de doelstellingen van de betrokken Unieregelgeving, moet worden vastgesteld dat de Raad en de Commissie, door voor te schrijven dat de namen van alle natuurlijke personen die steun ontvangen uit het ELGF en het ELFPO alsook de precieze door hen ontvangen bedragen moeten worden bekendgemaakt, de door het evenredigheidsbeginsel gestelde grenzen hebben overschreden.'

Verzoekers verwijzen naar het in deze materie belangrijke arrest van het EHRM van 4 december 2008 nrs. 30562/04 en 30566/04 inzake *S. and Marper t. Verenigd Koninkrijk,* (Idem, EHRM, 25 maart 1983, nr. 5947/72, inzake *Silver t. Verenigd Koninkrijk,* § 97; EHRM, *Malone t. Verenigd Koninkrijk,* (1984), Publications A82, § 84; EHRM, *Valenzuela Contreras t. Spanje,* (1998), Decisions and Reports 1998-V, § 47; EHRM, *P.G. and J.H. t. Verenigd Koninkrijk,* (2001), Decisions and Reports, 2001-IX, § 42; EHRM, *Sunday Times t. Verenigd Koninkrijk* (1979), Publications A30, §§ 49, 62, 65, 67;), waar bevestigd wordt dat het begrip 'noodzakelijk in een democratische samenleving' moet beantwoorden aan een 'pressing social need', en in het bijzonder dat het proportioneel moet zijn in verhouding tot het legitieme doel en dat de redenen opgegeven door de nationale overheden 'relevant en voldoende' moeten zijn. (overweging 101).

Het arrest stelt als besluit (overweging 125) dat '*the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, ... fails to strike a faire balance between the competing public and private intrests and that the respondent State has overstepped any acceptable margin of appreciation in this regard.'*

Eigen vertaling:
dat 'het blanco karakter en de willekeurige aard van de mogelijkheden tot het bijhouden van vingerafdrukken, speekselstalen en DNA profielen van verdachte maar niet veroordeelde personen, …, niet in overeenstemming is met de eerlijke balanstoets tussen de in het geding zijnde publieke en private belangen en dat de Staat op dit punt elke aanvaardbare grens van beoordeling heeft overschreden.'

In casu gaat het om de bewaring van (dikwijls gevoelige) communicatiegegevens van zelfs niet verdachte personen en dit zonder enig onderscheid tussen deze personen.

62.

A.2. De richtlijn 2006/24 heeft als doel de harmonisatie van de EU-wetgevingen gestoeld op de interne marktbeginselen van het Verdrag EU (artikel 114). De nationale implementatiewet, het hier bestreden artikel 5 van de wet van 30 juli 2013, stelt voornamelijk een politioneel doel te beogen ('vervolging strafbare feiten', artikel 126 § 2, a) en realiseert de facto (zonder er in de memorie ook maar iets over te zeggen) ook een doel van het vervullen van de inlichtingenopdrachten. De implementatie gaat bijgevolg, door een blanco-dataretentieverplichting op te leggen, veel verder dan het originele oogmerk van de richtlijn.

Op die wijze doorstaat het betwiste artikel niet de noodzakelijkheidstoets (en evenmin de proportionaliteitstoets).

In het kader van de eerste pijler had de EU in 2006 geen bevoegdheid om wetgeving op te leggen op het terrein van wethandhaving, met uitzondering van politiesamenwerking, justitiële samenwerking en harmonisering van strafwetgeving. (Advies advocaat-generaal EHJ, C-301/06, §§ 99, 100).

63.

A.3. Artikel 5 & 1 verplicht de aanbieders van telefoondiensten en internettoegang alle verkeersgegevens, locatiegegevens, gegevens voor identificatie van de eindgebruikers, gegevens voor identificatie van de vermoedelijke eindapparatuur te bewaren. Het artikel stelt verder dat geen gegevens bewaard mogen worden waaruit de inhoud van de communicatie kan worden opgemaakt.

De concrete toepassing van deze verplichting betekent dat van alle burgers vermelde gegevens bewaard worden, dit wil zeggen alle communicatiegegevens die via telefoon en internet

gegenereerd worden. In de moderne maatschappij verloopt 95% van de privé- en beroepscommunicatie op die wijze. De communicatie gebeurt vanuit de woning of de werkplaats. Telefoon en computer staan daar opgesteld. Het gaat om een gigantisch gebeuren van opslag, verwerking, toegang en openbaarmaking van die gegevens, die in veel gevallen ook heel gevoelige communicatiecontacten bevatten. Deze wetgeving houdt in dat intensief en massaal wordt binnengedrongen in het leven van alle burgers, waarvan de overgrote meerderheid nooit als schuldige voor een misdaad of wanbedrijf of voor een staatsgevaarlijke activiteit in aanmerking komt. Het gaat om een ingreep in de privacy die onze rechtsorde tot nu toe niet gekend heeft. De focus op wel precies omlijnde (potentiële) daders van misdrijven of staatsgevaarlijke elementen is volledig afwezig. De noodzaak van deze ingreep in een democratische samenleving is niet aangetoond. Verzoekers, die decennia lang opkomen voor het respect van de mensenrechten in België, benadrukken dat deze vraag naar noodzaak essentieel is in deze juridische discussie, met name welke grenzen wel of niet kunnen en mogen overschreden worden in een democratische maatschappij die maken dat het karakter van die maatschappij wezenlijk verandert. Historische voorbeelden leren dat een basisgegeven van dictaturen de totale controle op het privéleven van de burgers inhoudt.

Verzoekers stellen dat de bestreden wetgeving een fundamentele wijziging betekent in de verhouding tussen overheid en burger, waar in essentie alle communicatie via telefoon en internet van alle burgers onder controle wordt geplaatst. Dit is in strijd met de algemeen gedeelde opvatting in de Westerse democratieën dat de privacy aanzien wordt als een ‘afweerrecht’ van de burger tegen onverantwoorde indringing door de overheid in zijn of haar privéleven. Privacy, het recht op persoonlijke levenssfeer, behoort tot de kernvrijheden van die democratieën en werd in 1950 in het EVRM vastgelegd als reactie op de gebeurtenissen in de daarvoor liggende periode 1933-1945.

64.

In dat kader refereren verzoekers naar het arrest van het Duits Grondwettelijk Hof van 2 maart 2010 waarbij de Duitse wet die de omzetting was van de hier betwiste Richtlijn 2006/24 werd vernietigd omdat die bewaarplichtwet in strijd werd bevonden met het telecommunicatiegeheim dat in de Duitse Grondwet is vastgelegd. Het Duitse Grondwettelijk Hof kwalificeert de vernietigde wet als ‘een bijzonder zware ingreep tegen de rechten van de burgers met een reikwijdte die de rechtsorde tot nu toe niet gekend heeft. Het Hof stelt dat de wet ‘een verregaande inkijk in het sociale milieu en in de individuele activiteiten van de burgers toelaat’ en dat hij kan leiden ‘tot het opstellen van gedetailleerde persoonlijkheids- en verplaatsingsprofielen van vrijwel alle burgers.’ (Bundesverfassungsgericht, Urteil, 2 maart 2010, 1 BVR 256/08, 263/08, 586/08).

Verzoekers refereren eveneens naar de hoger geciteerde arresten van het Bulgaarse Administratieve Hof van 11 december 2011, van het Cypriotische Hooggerechtshof van februari 2011, van het Grondwettelijk Hof van Roemenië van 8 oktober 2009, van het Grondwettelijk Hof van de Tsjechische Republiek van 22 maart 2011.

Deze arresten vernietigden om redenen van ongrondwettigheid op grond van schending van het recht op privacy, het recht op informationele zelfbeschikking, van het briefgeheim, van de

vrijheid van meningsuiting, van de veiligheid en integriteit van telefonische- en postcommunicatie.

65.

Het gaat over een wezenlijke, 'bijzonder duidelijke' inmenging 'met een particulier karakter' in het privéleven. 'De betrokken gegevens, zo wil ik nogmaals benadrukken, zijn geen persoonsgegevens in de klassieke zin des woords die verband houden met precieze informatie over de identiteit van personen, maar in feite "gekwalificeerde" persoonsgegevens, die, wanneer zij worden geëxploiteerd, een belangrijk deel van het gedrag van een persoon, dat strikt onder zijn privéleven valt, op getrouwe en uitputtende wijze in kaart kunnen brengen of zelfs een volledig en precies beeld kunnen schetsen van zijn privé-identiteit.' (beschouwing 74 advocaat-generaal).

Zoals in het advies van de advocaat-generaal gesteld met betrekking tot de Richtlijn 2006/24, moet 'de kwaliteit van de wet' of 'het wettigheidsbeginsel' afdoende verzekerd worden, wat in casu niet het geval is.

Verzoekers stellen dat deze opslag in bulk op zich het wettigheidsbeginsel schendt. Er is, buiten de situatie van een noodtoestand, geen enkele 'dwingende maatschappelijke behoefte' (artikel 8 EVRM) denkbaar die een volledige opslag van alle vermelde gegevens van alle burgers zonder onderscheid kan verantwoorden. Door deze opslag wordt de 'wezenlijke inhoud' (artikel 52.1 Handvest) van het recht op privacy niet langer geëerbiedigd.

66.

In de memorie van toelichting wordt – opvallend – als enig motief voor het invoeren van de nieuwe wetgeving 'het cruciale belang voor de criminaliteitsbestrijding' aangehaald (Kamer, Parl. Stukken, Doc 53 2921/001 van 27 juni 2013, p. 16), hoewel het bestreden artikel veel verder gaat dan de criminaliteitsbestrijding. Conform artikel 8.2 EVRM is inmenging mogelijk in het kader van de openbare veiligheid of het voorkomen van strafbare feiten. Verzoekers stellen principieel dat er in een democratische maatschappij, behoudens uitzonderingstoestanden, geen noodzaak is om alle communicatiegegevens van alle burgers via telefoon of internet bij te houden, vanuit de doelstelling van de criminaliteitsbestrijding. In de memorie wordt gesproken over 'dé' criminaliteitsbestrijding; er wordt niet eens gerefereerd naar 'zware of ernstige criminaliteit', laat staan dat gerefereerd wordt naar specifieke misdrijven.

Minstens wordt in de wet en in de memorie niet 'voldoende precies, duidelijk en in nauwkeurige bewoordingen' bepaald in welke hypothesen de inmenging in het privéleven wordt voorzien. 'Dé' criminaliteit is een dermate ruim begrip dat ook misdrijven met bijvoorbeeld straffen beneden één jaar er kunnen onder vallen. De bepaling in de tekst dat het gaat om 'opsporing, onderzoek en vervolging van strafbare feiten zoals bedoeld in de artikelen 46bis en 88bis van het Wetboek van strafvordering', bevestigt ten overvloede het gebrek aan precisie en het gebrek aan verantwoording vanuit de noodzaak in een democratische samenleving. Het begrip 'strafbare feiten' zoals bedoeld in de artikels 46bis en 88bis die respectievelijk betrekking hebben op de bevoegdheid van de Procureur des Konings en de Onderzoeksrechter betreft alle misdaden en wanbedrijven, zonder enig onderscheid.

De aard en de omvang van de bewaarde gegevens schenden het recht op privacy.

Het is alleszins niet aangetoond dat artikel 5 van de wet van 30 juli 2013 beantwoordt aan een dwingende maatschappelijke behoefte, zodat het artikel in haar geheel dient vernietigd te worden.

B. De legaliteit van de wet is geschonden door niet twee naast elkaar bestaande regelingen op te zetten voor richtlijn 2002/58/EG en 2006/24/EG.

67.

Artikel 2 van de wet van 30 juli 2013 stelt dat de wet van 30 juli 2013 een omzetting is van zowel richtlijn 2006/24/EG als richtlijn 2002/58/EG.

De richtlijnen streven een ander doel na. Het verschil in doelstelling blijkt uit het volgende.

Richtlijn 2002/58/EG:
"Deze richtlijn harmoniseert 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 – 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 elektronische-communicatieapparatuur en diensten in de gemeenschap". (artikel 1, lid 1)

Richtlijn 2006/24/EG:
"Deze richtlijn heeft tot doel de bepalingen van de lidstaten te harmoniseren in verband met de verplichtingen van de aanbieders van openbaar beschikbare elektronische communciatiediensten of van openbare elektronischecommunciatienetwerken wat betreft de bewaring van bepaalde gegevens die door de aanbieders zijn gegenereerd of verwerkt teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de staten". (Artikel 1, lid 1)

68.

Het verschil in doelstelling tussen de twee richtlijnen wordt door de Raad van State ook aangehaald in haar advies van 27 mei 2013. Onder punt 3 stelt zij dat:

"Het Europees recht heeft zodoende een tweeledige regeling opgezet waarmee de operatoren inzake elektronische communicatie bepaalde gegevens bewaren:
– de ene regeling komt voort uit Richtlijn 2002/58/EG en biedt de lidstaten de mogelijkheid om de gegevensbewaring te regelen teneinde de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen of ervoor te zorgen dat strafbare feiten of onbevoegd gebruik van het elektronische-communicatiesysteem kunnen worden onderzocht, opgespoord en vervolgd;

– de andere regeling komt voort uit Richtlijn 2006/24/EG en streeft ernaar de verschillende nationale wetgevingen op elkaar af te stemmen teneinde te voorkomen dat de werking van de interne markt wordt belemmerd; ze verplicht de lidstaten een regeling voor gegevensbewaring in te voeren om te garanderen dat deze gegevens beschikbaar zijn om ernstig strafbare feiten zoals gedefinieerd in de nationale wetgevingen van de lidstaten (bijvoorbeeld georganiseerde misdaad en terroristische daden) te onderzoeken, op te sporen en te vervolgen".

Op pagina 33 van haar advies schrijft de Raad van State met verwijzing naar de evaluatie van 18 april 2011 van de Commissie dat het voorstelde artikel 126 beduidend verder reikt dan de doelstellingen bepaald in richtlijn 2006/24/EG. De Raad van State stelt in punt 4 dan ook voor om twee naast elkaar bestaande regelingen op te zetten:

> "*Uit de voorgaande overwegingen blijkt dat de lidstaten op basis van richtlijn 2002/58/EG regelingen kunnen opzetten die de operatoren verplichten gegevens te bewaren met oogmerken die verder reiken dan het oogmerk bepaald door richtlijn 2006/24/EG, met naleving evenwel van bepaalde voorwaarden die zijn vastgesteld door artikel 15 van richtlijn 2002/58/EG.*
> *Dat is de regeling die door het ontworpen artikel 126 in aanmerking wordt genomen: deze bepaling zet niet alleen richtlijn 2006/24/EG om, maar beantwoordt bovendien aan en vindt steun in artikel 15 van richtlijn 2002/58/EG in zoverre ze verder reikt dan de doelstelling in verband met de "ernstige criminaliteit" die door deze richtlijn wordt aangegeven.*
> *Desalniettemin, gelet op de complexiteit van het Europees recht en, om de bewoordingen van de Europese Commissie aan te halen, gelet op "dit ingewikkelde juridische verband" tussen richtlijn 2006/24/EG en richtlijn 2002/58/EG, kan men zich afvragen of de beste oplossing om te garanderen dat het Europees recht wordt nageleefd er niet in bestaat twee naast elkaar bestaande regelingen op te zetten: een regeling die richtlijn 2006/24/EG omzet en een andere regeling die op richtlijn 2002/58/EG steunt. In dit verband merkt de afdeling Wetgeving voorts op dat in overwegingen 15 en 16 van de aanhef van richtlijn 2006/24/EG wordt vermeld dat "de Richtlijnen 95/46/EG en 2002/58/EG integraal van toepassing zijn op de overeenkomstig (...) richtlijn [2006/24/EG] bewaarde gegevens".*
> *Hoe het ook zij, daar de steller van het voorontwerp heeft gekozen voor een regeling die op de twee voornoemde richtlijnen steunt, moet hij het tweeledige juridisch kader naleven waarop hij zich beroept.*
> *In de bijzonder opmerkingen die hierna volgen, wordt met dit vereiste rekening gehouden.*"

Op pagina 36 stelt de Raad van State in verband met het artikel 126:

> "*In verband met de overdracht van de gegevens die zal plaatsvinden krachtens het ontworpen artikel 126, § 2, eerste lid, b) en c), wordt in de ontworpen tekst en in de wetsbepalingen waarnaar wordt verwezen, evenwel niets gezegd over de overheidsinstanties en, bovenal, evenmin over de precieze regels voor het aanvragen en overdragen van de gegevens.*
> *De artikelsgewijze toelichting bevat geen bijkomende uitleg.*

Aangezien het een regeling betreft die strijdig kan zijn met een grondrecht, te weten de bescherming van de persoonlijke levenssfeer, moet de wetgever zelf de kernpunten van de regeling inzake deze overdracht vastleggen. De ontworpen tekst moet dienovereenkomstig worden aangevuld."

De tekst werd niet aangevuld ondanks het advies van de Raad van State. Er werden geen precieze regels vastgelegd in de wet voor het aanvragen en overdragen van de gegevens.

69.

Op basis van het advies van de Raad van State wordt gesteld dat de kwaliteit van de wet niet voldoet op twee aspecten:

-De wetgever is het advies van de Raad van State om twee afzonderlijke wetgevingssytemen te maken niet gevolgd. De vermenging in de wet van de omzetting van twee richtlijnen met verschillende doelstellingen leidt tot een 'ingewikkeld juridisch verband' dat het Europees recht geformuleerd in de twee richtlijnen niet naleeft; dit leidt tot een vernietiging van het ganse artikel 5 van de wet van 30 juli 2013.

-Door niets te bepalen over de bevoegde overheden en de precieze regels voor aanvragen en overdracht wordt de legaliteit geschonden; dit betreft artikel 126 § 2, eerste lid b) en c). Verzoekers zijn evenwel van mening dat dit wat de precieze regels voor aanvraag en overdracht ook artikel 126 § 2, eerste lid a) en d) betreft.
De bepaling dat de overdracht 'onverwijld' en 'op eenvoudig verzoek' gebeurt (artikel 126 §2, laatste alinea) beantwoordt niet aan de noodzaak van precieze regel.

C. Schending van legaliteit en proportionaliteit door artikel 126, § 2, d

70.

Artikel 126 § 2 onder d, wet van 2005 bepaalt:
"d) de vervulling van de inlichtingenopdrachten met inzet van de methoden voor het verzamelen van gegevens zoals bedoeld in de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten."

Krachtens de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (verder genoemd BIM-wet) kan het diensthoofd – wanneer dit een belang vertoont voor de uitoefening van de opdrachten – bij schriftelijke of mondelinge beslissing de medewerking van een elektronisch communicatienetwerk of van een elektronische communicatiedienst vorderen inzake het verstrekken van communicatie- dan wel identificatiegegevens.

71.

De opdrachten van de Veiligheid van de Staat zijn als volgt gedefinieerd:

– “De Veiligheid van de Staat heeft als opdracht: 1º het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door het Ministerieel Comité, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van het Ministerieel Comité,
bedreigt of zou kunnen bedreigen”. (artikel 7 BIM-wet)

– “Voor de toepassing van artikel 7 wordt verstaan onder: 'activiteit die bedreigt of zou kunnen bedreigen': elke individuele of collectieve activiteit ontplooid in het land of vanuit het buitenland die verband kan houden met spionage, inmenging, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties, criminele organisaties, daarbij inbegrepen de verspreiding van propaganda, de aanmoediging of de rechtstreekse of onrechtstreekse steun, onder meer door het verstrekken van financiële, technische of logistieke middelen, het
verstrekken van inlichtingen over mogelijke doelwitten, de ontwikkeling van structuren en van actiecapaciteit en de verwezenlijking van de nagestreefde doeleinden. (artikel 8 BIM-wet)

– “Voor de toepassing van het vorige lid wordt verstaan onder:(...) c) extremisme: racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, ongeacht of ze van politieke, ideologische, confessionele of filosofische aard zijn, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat”. (artikel 8 BIM-wet)

– “De specifieke methoden voor het verzamelen van gegevens zijn: (…) 5º de maatregelen tot opsporing van de oproepgegevens van elektronische communicatiemiddelen en de lokalisatie van de afkomst of de bestemming van elektronische communicatie”. (artikel 18/2 BIM-wet)

– “De specifieke methode kan slechts worden aangewend na een schriftelijke en met redenen omklede beslissing van het diensthoofd en na kennisgeving van deze beslissing aan de commissie”. (artikel 18/3 BIM-wet)

72.

Bovenstaande wetgeving gelezen in combinatie met artikel 5 van de wet van 30 juli 2013 en inzonderheid met artikel 126 § 2, d leidt tot situaties waarbij de rechtszekerheid en het verbod van willekeur in het geding komen en de inmenging van de overheid in de privacy, maar ook in het recht op vrije meningsuiting en eredienst (artikel 19 G.W.), in de vrije drukpers (artikel 25 G.W.), in het recht op vergadering (artikel 26 G.W.) en op vereniging (artikel 27 G.W.) op een niet proportionele wijze worden aangetast.

Het werkterrein van de inlichtingen- en veiligheidsdiensten is zeer ruim omschreven. De dataretentie die door de wet wordt ingevoerd betreft de communicatiedata van alle burgers en deze worden twaalf maanden bewaard. De methode van het inzamelen van communicatiedata is voor de inlichtingen- en veiligheidsdiensten een specifieke methode, die op eenvoudige vraag van

het diensthoofd kan geschieden en dit zonder toestemming van de Commissie van magistraten. De combinatie van deze twee wettelijke regelingen maakt dat op eenvoudige vraag van het diensthoofd met een terugwerkende kracht van twaalf maanden alle telefoon- en internetdata kunnen worden opgevraagd van wie onder één van de kwalificaties van de bevoegdheden van de staatsveiligheid valt. Er dient hierbij onderlijnd dat de gecombineerde regeling van de hier bestreden wet en van de toepasselijke artikels van de wet op de inlichtingen- en veiligheidsdiensten geen onderscheid maakt tussen de verschillende activiteiten die tot de opdracht van die diensten behoort, terwijl deze activiteiten zeer uiteenlopend zijn en bepaalde opvattingen of bedoelingen voor veel interpretatie vatbaar zijn, naar gelang de politieke of maatschappelijke invulling die het diensthoofd er aan geeft.

Verzoekers menen dat de wet zoals thans gesteld tot machtsmisbruik kan leiden opzichtens individuen of organisaties die kritisch staan tegenover de regering of tegenover het politieke systeem.

Hetzelfde gevaar stelt zich voor de persvrijheid, daar de wet de inlichtingen- en veiligheidsdiensten toelaat met terugwerkende kracht van twaalf maanden alle telefonische- en internetcommunicatie van journalisten op te vragen, dus ook van zij die een artikel of onderzoek hebben gedaan dat gekwalificeerd zou worden in het brede kader van de opdrachten van die diensten.

De wet zal ook tot zelfcensuur van burgers aanleiding geven. Er mag niet worden voorbijgegaan aan het vage gevoel gecontroleerd te worden dat de wet kan veroorzaken, een bepalende invloed kan hebben op de uitoefening door de Europese burgers van hun vrijheid op meningsuiting en informatie, en zo een inmenging betekent op artikel 11 van het Handvest (beschouwing 52 advocaat-generaal). De rechtspraak is niet ongevoelig gebleven voor deze zogenoemde „chilling effect" doctrine (afschrikkende werking) (US Supreme Court, Wiemann/Updegraff, 344 US 183 (1952); EHRM, arrest van 25 oktober 2011, *Altuğ Taner Akçam/Turquie,* klacht nr. 27520/07, § 81; zie met name „The Chilling Effect in Constitutional Law", *Columbia Law Review*, 1969, deel 69, nr.5, blz. 808).

Verzoekers stellen dat een dergelijke ruime delegatie van bevoegdheid van overdracht en inzage in data in het kader van de hier bestreden wet op de dataretentie de kwaliteit van de wet schendt, alleszins disproportioneel is. Er had minstens in de wet een onderscheid dienen aangeduid te worden voor welke opdrachten van de inlichtingen- en veiligheidsdiensten de data wel konden opgevraagd worden.

Artikel 126 §1, §2,d, §3 ingevoerd door artikel 5 van de wet van 30 juli 2013 zijn strijdig met het legaliteits- en proportionaliteitsbeginsel in dienen vernietigd te worden.

D. De wet is onvoldoende precies in zijn bewoordingen wat betreft de beoordelingsbevoegdheden van de betrokken overheden.

73.

De inmenging voldoet niet aan het wettigheidsbeginsel daar de wet onvoldoende duidelijk de beoordelingsbevoegdheid van de betrokken overheden afbakent. Dit geldt minstens en inzonderheid voor wat betreft de overheden aangeduid onder punten a en d van artikel 126 § 2, met name respectievelijk inzake opsporing, onderzoek en vervolging van strafbare feiten en de inlichtingenopdrachten van de Staatsveiligheid en de Veiligheid van het Leger.

Wat artikel 126 § 2, a betreft wordt er niet eens een overheid aangeduid; er worden wel 'strafbare feiten' aangeduid die verwijzen naar de bevoegdheid van de Procureur des Konings en de Onderzoeksrechter, doch in het kader van die bevoegdheden kunnen ook andere overheden zoals bijvoorbeeld politieofficieren, sociale inspecties en dergelijke optreden.
Een specifieke afbakening van de bevoegdheden van de Procureur des Konings en de Onderzoeksrechter is alleszins niet aanwezig.

Wat artikel 126 § 2, d betreft worden niet direct de beoordelingsbevoegdheden van de vermelde inlichtingendiensten vermeld, maar enkel de inlichtingenopdrachten zelf wat een ander begrip is dan de beoordelingsbevoegdheid van die diensten. Het kader wordt afgebakend door de methoden bepaald in artikel 18/7 en 18/8 van de wet van 30 november 1998, waaruit dan indirect een bevoegdheidsbeoordeling zou kunnen afgeleid worden, namelijk deze van het diensthoofd. Maar ook hier ontbreekt in de wet zelf een precieze en voldoende duidelijke bevoegdheidsomschrijving en beoordelingsbevoegdheid.

Zoals uit het advies van de advocaat-generaal bij het Europees Hof van Justitie mag blijken volstaat een verwijzing naar de algemene bevoegdheden van wetshandhavingsinstanties en veiligheidsdiensten niet. Dergelijke verwijzing is precies de miskenning van de ratio legis die van de nieuwe wetgeving uitgaat. Het gaat niet om een eenvoudige aanpassing of aanvulling van reeds bestaande bevoegdheden, maar het gaat om een constitutionele wijziging met betrekking tot de privacy van de burgers (beschouwing 121, 123) en een afwijking van de beginselen die vastgelegd zijn in de twee richtlijnen 95/46/EG en 2002/58/EG (beschouwing 39). Het gaat over een wezenlijke, 'bijzonder duidelijke' inmenging 'met een particulier karakter' in het privéleven, die 'een belangrijk deel van het gedrag van een persoon, dat strikt onder het privéleven valt, op getrouwe en uitputtende wijze in kaart kan brengen of zelfs een volledig en precies beeld kan schetsen van zijn privé-identiteit' (beschouwing 74).

De artikels 126, § 2 a en d dienen vernietigd te worden.

E. De wet voorziet geen afdoend jurisdictioneel toezicht tegen willekeurige aantasting door de overheid.

74.

De wet voldoet niet aan 'kwaliteit van de wet' daar het opslaan/vernietiging van de gegevens en de controle op de beveiliging ervan volledig wordt overgelaten aan de aanbieders van een netwerk of dienst voor elektronische communicatie. (artikel 126 § 1 en § 5).

Wat de opslag en vernietiging van de data betreft is er geen enkel controlemechanisme ingesteld.

Enkel wat de toegang tot de gegevens betreft voorziet de wet dat dit gebeurt door leden van de Coördinatiecel Justitie. (artikel 126 § 5, 3°).

Het advies van de advocaat-generaal bij het Europees Hof van Justitie merkt in dit verband terecht op dat 'de intensiteit van de inmenging des te duidelijker wordt door factoren die het risico vergroten…'. 'Deze gegevens worden namelijk niet bewaard door de autoriteiten zelf of zelfs maar onder hun directe toezicht, maar door de aanbieders van elektronische communicatiediensten, op wie het merendeel van de verplichtingen rust die als waarborg van de bescherming en de veiligheid van de gegevens moeten dienen'. En verder: '… geen enkele bepaling die deze dienstenaanbieders verplicht de gegevens zelf te bewaren op het grondgebied van de lidstaat, dat onder de rechtsmacht van een lidstaat valt, hetgeen het risico dat zij in strijd met deze regeling toegankelijk of openbaar gemaakt worden, aanzienlijk vergroot'. 'Door deze "outsourcing" … wordt het risico vergroot dat de gegevens worden geëxploiteerd op een wijze die niet in overeenstemming is met de eisen die voortvloeien uit het recht op eerbiediging van het privéleven.' (beschouwingen 74-79). De recente onthullingen over de praktijken van de NSA en BGHC en anderen maakt het door de advocaat-generaal geschetste gebrek aan kwaliteit van de wet, wel heel pertinent.

75.

Artikel 126 § 1 stelt dat het geldt 'onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens'. Er wordt mogelijk opgeworpen dat deze bepaling voldoende kwaliteit geeft aan de wet in het kader van de waarborgen tegen willekeurige aantastingen van de privacy. Deze wet en de latere aanpassingen zijn de realisatie en omzetting in België van de Richtlijn 95/46/EG en 2002/58/EG. Het advies van de advocaat-generaal bij het Europees Hof van Justitie stelt terecht dat de Richtlijn 2006/24 een 'diepgaande wijziging van de stand van het recht dat van toepassing is op gegevens in verband met elektronische communicatie en voortvloeit uit de richtlijnen 95/46 en 2002/58' meebrengt en derhalve 'een regeling invoert die afwijkt van de beginselen' van deze twee richtlijnen (beschouwingen 37 en 39). De wet van 8 december 1992 is bijgevolg geen voldoende garantie. Opnieuw dient benadrukt dat de hier bestreden Belgische wet niet een eenvoudige wijziging meebrengt aan de verhouding tussen overheid en de privacy van de burgers, maar 'een diepgaande' wijziging meebrengt. Het is precies dit wezenlijke verschil dat gepaard gaat met de nieuwe wet vergeleken met al de voorgaande inmengingen in de privacy dat aan de wetgever ontsnapt is, zoals de memorie van toelichting en de debatten in Kamer en Senaat vermogen te illustreren. Advocaat-generaal bij het Hof van Justitie formuleert dit kwalitatief en kwantitatief verschil zeer precies: '*De betrokken gegevens, zo wil ik nogmaals benadrukken, zijn geen persoonsgegevens in de klassieke zin des woords die verband houden met precieze informatie over de identiteit van personen, maar in feite "gekwalificeerde" persoonsgegevens, die, wanneer zij worden geëxploiteerd, een belangrijk deel van het gedrag van een persoon, dat strikt onder zijn privéleven valt, op getrouwe en uitputtende wijze in kaart kunnen brengen of zelfs een volledig en precies beeld kunnen schetsen van zijn privé-identiteit.*' (beschouwing 74).

Het is precies ook vanuit die ratio legis dat de advocaat-generaal met betrekking tot de richtlijn heeft gesteld dat deze in strijd is met artikel 52 (1) van het Handvest omdat zij geen reeks

principiële waarborgen voorziet en een algemene verwijzing naar de lidstaten niet volstaat. 'Principiële waarborgen zijn een noodzakelijk en onmisbaar complement' van de richtlijn. (beschouwing 123). Deze noodzakelijke en onmisbare waarborgen zijn in de hier bestreden Belgische wet ook volledig afwezig.

De advocaat-generaal stelt in beschouwing 113 dat de moeilijkheid van richtlijn 2006/24 precies is ('ik herhaal het nog maar eens') dat ze 'niet de waarborgen regelt die de toegang tot deze bewaarde gegevens en de exploitatie ervan moeten beheersen'.

Ook in de hier bestreden wet zijn deze specifieke waarborgen niet aanwezig. De waarborgen die uit andere wetgevingen kunnen afgeleid worden, quod non, beantwoorden niet aan specifieke waarborgen die in verhouding staan tot de kwaliteit en kwantiteit van de ingreep op de privacy die de wet realiseert.

76.

Artikel 126 § 5 voldoet niet aan de wettigheidsvereiste voor wat betreft de noodzaak om een voldoende jurisdictioneel toezicht te voorzien als waarborg tegen willekeur.

De verantwoordelijkheid wordt volledig bij de aanbieder van het netwerk of van de dienst voor elektronische communicatie gelegd. Het invoeren bij KB van technische en administratieve maatregelen zoals voorzien in artikel 126 § 5 is een technische maatregel maar is geen toezichtmaatregel, laat staan een jurisdictioneel of extern toezicht. De tussenkomst van de leden van de Coördinatiecel Justitie betreft enkel de toegang tot de bewaarde gegevens en niet de opslag, bewaring en vernietiging ervan. Bovendien zijn de leden van die Coördinatiecel geen externe toezichters, maar personen die zelf behoren tot de providers of telecommaatschappijen.

Artikel 5 in haar geheel dient vernietigd te worden, minstens en alleszins de onderdelen die met artikel 126 § 1 en 5 worden ingevoerd.

F. Het begrip 'strafbare feiten' beantwoordt niet aan het principe van legaliteit, is alleszins niet evenredig.

77.

Meer specifiek wordt gesteld dat het begrip 'vervolging van strafbare feiten' niet beantwoordt aan het principe van legaliteit, alleszins niet aan het principe van de evenredigheid. (artikel 126, § 2, a)

Het heeft voor gevolg dat alle wanbedrijven en misdaden de basis kunnen vormen voor niet enkel de bewaring maar ook het exploiteren van de bewaarde persoonsgegevens.

De legaliteit vereist dat precies wordt aangeduid voor welk soort misdrijven een dergelijke verregaande inmenging in de privacy gerechtvaardigd is. De advocaat-generaal bij het Europees

Hof van Justitie stelt terecht dat ‘rekening houdend met de intensiteit van de inmenging, een duidelijke omschrijving had moeten gegeven worden van de criminele activiteiten die de toegang van de bevoegde nationale overheden tot de verzamelde en bewaarde gegevens zouden rechtvaardigen. Het moet gaan om een grotere graad van precisering dan enkel het begrip “zware inbreuken”. (beschouwing 126). Dezelfde redenering gaat volledig op voor de hier bestreden wet. Ze geldt nog des te meer daar de wet zelfs niet het begrip “zware inbreuken” hanteert, maar wel “strafbare feiten”, wat nog veel ruimer is. Ze geldt verder nog des te meer daar ze niet beantwoordt aan de door de advocaat-generaal op zichzelf reeds gekritiseerde gehanteerde begrip ‘ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de staten’ (Artikel 1 Richtlijn 2006/24).

78.

Het is niet evenredig om voor alle wanbedrijven en misdaden de verplichting tot bewaring op te leggen. Het is niet evenredig om voor alle wanbedrijven en misdaden zonder onderscheid aan de Procureur des Konings en aan de Onderzoeksrechter de mogelijkheid te geven inzage te nemen van persoonsdata inzake communicatie over een periode van 12 maanden.

Zoals én in het advies van de advocaat-generaal gesteld én in de evaluatie van de Europese Commissie dient een ‘beperking van de doelen’ en van ‘de types criminaliteit’ waarvoor de data kunnen bewaard en opgevraagd worden in de wet zelf te worden opgenomen.

Artikel 126 § 2, a dient bijgevolg te worden vernietigd.

G. Geen definitie van de te bewaren gegevens per type noch wat betreft de vereisten waaraan deze gegevens moeten beantwoorden.

79.

Artikel 126 § 1 stelt dat bij Koninklijk Besluit zal vastgesteld worden de te bewaren gegevens per type alsook de vereisten waaraan deze gegevens moeten beantwoorden.

De te bewaren gegevens en de kwaliteit waaraan zij moeten beantwoorden zijn dermate bepalend dat zij niet kunnen worden overgelaten aan de uitvoerende macht, daar zij van vandaag op morgen kunnen gewijzigd worden. Dit kan leiden tot willekeur en machtsmisbruik.

Minstens het specifieke onderscheid tussen identificatie-data en communicatie-data diende in de wet te worden ingeschreven, temeer omdat voor de eerste categorie in feite een onbeperkte bewaringstermijn (tot 12 maanden na laatste communicatie) is voorzien.

De in hetzelfde artikel vermelde data zijn niet proportioneel daar zij alle elementen van identificatie en alle data van communicatie omvatten, met inbegrip van EMS (enhanced media service) en MMS (multimedia service), wat bijvoorbeeld ook abonnees op diensten en zenders van televisie … inhoudt. Er is geen verantwoording voor het bewaren van in feite alle data die via internet of telefoon gegenereerd worden.

Dit gaat het vooropgestelde doel 'vervolging strafbare feiten' ver te buiten.

De wet is ook onduidelijk wat betreft het onderscheid tussen '*trafic data*' en '*content data*'. In het vermelde artikel worden deze door mekaar gebruikt.

Artikel 126 § 1 schendt zowel legaliteit als proportionaliteit.

H. De bewaringstermijn beantwoordt niet aan de voorwaarden van legaliteit en proportionaliteit.

80.

Verzoekers verwijzen hiervoor naar wat gesteld is onder punt 60, dat hier voor herhaald wordt aanzien.

Er zijn twee bewaringstermijnen bepaald in de wet: één voor de identificatiegegevens, en één voor de communicatiegegevens.

Wat de identificatiegegevens betreft gaat het in feite om een onbeperkte termijn, die begint te lopen vanaf de aansluiting en loopt tot twaalf maanden na de laatste communicatie.

De Raad van State heeft hierbij terecht volgende bedenking gemaakt:

"*De logica van de aldus geformuleerde rechtvaardiging valt te begrijpen, maar de vraag rijst of met de regeling die hier wordt opgezet in sommige gevallen de termijn voor de gegevensbewaring, zoals die naar voren komt wanneer de artikelen 5 en 6 van richtlijn 2006/24/EG in onderling verband wordt gelezen, niet wordt overschreden*." (Memorie van Toelichting, p. 38).

Wat de communicatiegegevens betreft laat de wet toe dat de bewaringstermijn tot 18 maanden verlengd wordt bij KB, maar dat na evaluatie zelfs een langere periode wordt ingevoerd.

Uit de memorie van toelichting blijkt dat de bewaringstermijn 'vandaag evenwel op 12 maanden is vastgelegd', maar het is duidelijk dat dit als een overgangssituatie wordt aanzien om thans de wet te realiseren tegen de bezwaren in van de elektronische-communicatiesector en de Privacycommissie en het de bedoeling is om na twee jaar een langere bewaartermijn in te stellen (Memorie van Toelichting, p. 17).

Tweede middel

Artikel 5, 10 en 11 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden en artikel 2 van het 4de aanvullende protocol bij het EVRM;
Artikel 9, 12 en 19 van het Internationaal Verdrag inzake Burgerrechten en Politieke rechten
Artikel 10, 11, 12, 19, 25, 26 en 27 van de Gecoördineerde Grondwet;
Het beginsel van proportionaliteit;

GESCHONDEN REFERENTIENORMEN – Recht op persoonlijke vrijheid en vrije meningsuiting en het recht op vrijheid van vergadering en vereniging, al dan niet in samenhang gelezen met het recht op bronnengeheim en beroepsgeheim en het beginsel van proportionaliteit:

1. **Aangevochten beschikkingen van de bestreden wet**

81.

Zie eerste middel, punt 40.
Dit wordt hier voor herhaald aanzien.

2. **Het onderzoekskader**

82.

Zie eerste middel, punt 41-43.
Dit wordt hier voor herhaald aanzien.

3. **Grieven**

Eerste onderdeel

Samenvatting van het middelonderdeel

Bewaren van verkeersgegevens heeft een verstorend effect op vrije expressie van informatie en ideeën en op de persvrijheid.

Het recht op vrije meningsuiting en de vrije pers worden zowel grondwettelijk als verdragsrechtelijk beschermd.

83.

Artikel 19 G.W. 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 10, §1 EVRM bepaalt:

"*Een ieder 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 te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen*."

De macht om maatregelen te nemen die een impact hebben op de vrije meningsuiting is beperkt en ondergeschikt aan het belang van de fundamentele rechten vervat in de Grondwet en het Europees verdrag voor de rechten van de mens.

Krachtens artikel 10, §2 EVRM kan het recht op vrije meningsuiting door de overheid slechts worden ingeperkt indien het in het licht van de welbepaalde omstandigheden van elk geval bewezen is dat er dwingende redenen zijn om dit recht in te perken.

Dwingende redenen zullen voorhanden zijn indien de uitoefening van het recht op vrije meningsuiting in conflict zou komen met andere door het EHRM gewaarborgde rechten, die primeren.

Ook redenen van ordehandhaving kunnen dwingende redenen uitmaken. Hier kan worden gedacht aan de inzet van bijzondere opsporingsmethoden om bepaalde vormen van criminaliteit, in het bijzonder zware misdaden of misdaden die worden gepleegd door criminele organisaties die over aanzienlijke middelen beschikken, te bestrijden. Bijzondere opsporingsmethoden, zoals een internettap of een telefoontap, maakt zonder de minste twijfel een aantasting van het recht op vrije meningsuiting uit.

Het EHRM aanvaardt de toelaatbaarheid van deze onderzoeksmethoden en deze principiële toelaatbaarheid wordt door de bewaarplicht uit bestreden wet niet gewijzigd. Het EHRM eist evenwel op grond van artikel 6 EVRM in haar rechtspraak bijzondere garanties.[16] Uit de rechtspraak van het EHRM volgt dat machtigingen inzake bijzondere opsporingsmethoden voldoende precieze gegevens moeten bevatten opdat de betrokkenen en de rechter eventuele misbruiken zouden kunnen opsporen.[17] Een bijzondere opsporingsmethode die is uitgevoerd zonder wettelijke grondslag en zonder afdoende garanties kan geen geldig bewijs opleveren.[18]

De aard of de ernst van het misdrijf vormen geen rechtvaardiging voor de beperking van het recht op vrije meningsuiting.

[16] EHRM Ramanauskas t. Litouwen, 2008, overweging 53; EHRM Khoudobine t. Rusland, 2006, overweging 135.
[17] EHRM Ramanauskas/Litouwen van 5 februari 2008, overweging 53; EHRM Khoudobine t. Rusland, 2006, overweging 135.
[18] EHRM Ramanauskas t. Litouwen, 2008, overweging 60.

84.

Artikel 5, § 2 van bestreden wet bepaalt:

"§ 2. De gegevens bedoeld in paragraaf 1, eerste lid, worden bewaard met het oog op :

a) de opsporing, het onderzoek en de vervolging van strafbare feiten zoals bedoeld in de artikelen 46bis en 88bis van het Wetboek van strafvordering;

b) de beteugeling van kwaadwillige oproepen naar de nooddiensten, zoals bedoeld in artikel 107;

c) het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of -dienst, zoals bedoeld in artikel 43bis, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

d) de vervulling van de inlichtingenopdrachten met inzet van de methoden voor het verzamelen van gegevens zoals bedoeld in de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de gegevens opgenomen in paragraaf 1, eerste lid, onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en op eenvoudig verzoek aan de autoriteiten belast met de opdrachten bedoeld in de punten a) tot d) kunnen worden meegedeeld en uitsluitend aan deze laatsten".

De categorieën "*de beteugeling van kwaadwillige oproepen naar de nooddiensten"* en *"het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of -dienst"* en "*de vervulling van de inlichtingenopdrachten"* gaan evenwel verder dan de door de richtlijn geformuleerde doelstelling, zijnde de opsporing en beteugeling van strafbare feiten.

Aan vier zeer uiteenlopende diensten wordt de mogelijkheid geboden om gedurende twaalf maanden bewaarde communicatiegegevens en gedurende in principe onbeperkte tijd (tot na een jaar na de laatste communicatie) bewaarde identiteitsgegevens op te vragen.

Welke diensten bedoeld zijn onder artikel 126 § 2 a, b en d is zelfs niet aangeduid, en zou moeten gededuceerd worden door de burger uit wat impliciet zou kunnen begrepen worden. Enkel de dienst onder 126 § 2 c is aangeduid als 'Ombudsdienst voor telecommunicatie'.

Er kan eventueel gededuceerd worden dat de Procureur des Konings, de politiediensten, de Onderzoeksrechter, de diensthoofden van Staatsveiligheid en de Veiligheid van het leger, en eventueel ook de Ombudsdienst voor telecommunicatie en de telefonische nooddiensten (welke dit ook moge zijn) de bewaarde persoonsgegevens kunnen opvragen.

Daarnaast is ook de opslag zelf van een gigantisch groot aantal identificatie- en communicatiegegevens door providers en telecomoperatoren een element voor vrees voor inbreuk op de vrije expressie, op de vrije informatiewinning en op de persvrijheid.

Verzoekers verwijzen naar wat reeds werd ontwikkeld in het eerste middel met betrekking tot de ontoereikendheid van de beschermings- en controlemechanismen met betrekking tot zowel de opslag als de inzage van de persoonsgegevens.

Zoals in het eerste middel ook aangegeven, en hier voor herhaald aanzien, zijn de legaliteit en de proportionaliteit niet verzekerd zowel wat betreft de gegevens die bewaard en ingekeken kunnen worden met betrekking tot 'vervolging van strafbare feiten' als met betrekking tot de ruime bevoegdheden van de twee Belgische inlichtingen- en veiligheidsdiensten.

De bestreden wet omschrijft niet wat moet worden begrepen onder "vervolging van strafbare feiten" en ook in de memorie van toelichting wordt geen rechtvaardiging voor of invulling van het begrip gegeven.

Aldus uitgelegd en gezien de loutere 'vervolging' van 'strafbare feiten' een dwingende reden kunnen uitmaken die een beperking op het recht op vrije meningsuiting kan rechtvaardigen, schendt de bestreden wet alle in het middel aangehaalde referentienormen.

85.

In de moderne maatschappij is telecommunicatie niet meer denkbaar zonder dat gebruik wordt gemaakt van databanken waarin persoonsgegevens worden gekoppeld met elektronische adresgegevens om de juiste routering en bestemming van een boodschap tot stand te brengen. Er treedt een vermenging op van individuele communicatieve handelingen en het waarnemen en vastleggen van persoonsgegevens. Hierdoor raakt het informationele privacyrecht in sterkere mate dan nu het geval is verweven met het communicatiegeheim.

Terwijl artikel 10 Grondwet toeziet op de bescherming van de persoonlijke levenssfeer, ziet het transportgeheim toe op de betrouwbaarheid van het communicatiekanaal. Geheimhouding van verkeersgegevens dient deze betrouwbaarheid. Het gaat er dan ook niet enkel over dat verkeersgegevens veel over personen kunnen zeggen, belangrijk is ook dat het vertrouwen dat de burger stelt in het communicatiekanaal kan worden aangetast, wanneer verkeersgegevens worden verwerkt voor doelen die niet noodzakelijkerwijs voortvloeien uit het leveren van de dienst. Wanneer de burger er rekening mee moet houden dat wordt bijgehouden met wie hij wanneer en hoe lang communiceert en vervolgens deze informatie buiten het kader van de dienst voor allerlei doeleinden wordt verwerkt, zal hij niet meer vrij kunnen communiceren.[19]

[19] L. Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*', Amsterdam Otto Cramwinckel Uitgever, 2002.

86.

In een arrest van het Bundesverfassungsgericht van 15 december 1983[20] sprak het Duitse Grondwettelijk Hof zich uit over het belang van een democratisch communicatiesysteem om de fundamenteel bevonden vrijheid van meningsuiting, het recht op privacy en persoonlijke vrijheid te vrijwaren:

"*In modern society characterized among others by enormous rise in the amount of information and data, individuals have to be protected against unlimited collection, retention, use and disclosing of data concerning one's person and privacy within the scope of a more general right of an individual to privacy guaranteed by the constitution. Should individuals not be guaranteed the possibility to guard and control the contents as well as scope of personal data and information provided which are to be disclosed, retained or use for other than their original purposes, should they not have the possibility to identify and access reliability of their potential communication partners and adjust their actions accordingly, then this is inevitably a case of infringement or restriction of their rights and freedoms and therefore, one can in such case not speak of a free and democratic society."*

Eigen vertaling:
"In de moderne maatschappij die onder meer gekenmerkt wordt door de enorme toename van informatie en data, moeten de individuen beschermd worden tegen onbegrensde opslag, bewering, gebruik en ontsluiten van data die hun privéleven betreffen, en dit vanuit het standpunt van het meer algemeen recht op bescherming van het privéleven zoals in de grondwet vastgelegd. Wanneer individuen geen garantie hebben dat zij toezicht en controle kunnen houden zowel op de inhoud als op het gebruik van persoonsgegevens en informatievoorziening dat die voor hun oorspronkelijk doel dienen bekeken, weerhouden en gebruikt worden, wanneer zij niet de mogelijkheid hebben de potentiële partners van hun communicatie en de daarmee verbonden activiteiten te identificeren en er effectieve toegang toe te hebben, dan is dat ongetwijfeld een inmenging in en een beperking van hun vrijheden en om die reden kan in die omstandigheden niet gesproken worden van vrijheid van mening en van een democratische maatschappij."

In latere rechtspraak oordeelt het Duits Grondwettelijk Hof hierover dat de bewaarplicht een bedreiging van de vrije informatieve-uitwisseling en het vertrouwen in het communicatiegeheim impliceert.[21] Ook benadrukt het Duits Grondwettelijk Hof dat dataretentie een zogenaamd "*chilling effect*" heeft: het verhindert het op legitieme wijze ongehinderd gebruikmaken van telecommunicatie door burgers, uit angst voor daaruit voortvloeiende strafprocesrechtelijke maatregelen.[22] Dit *chilling effect* wordt volgens het Hof versterkt door de omstandigheid dat de opslag voor het individu niet waarneembaar is.

Breyer meent dat het *chilling effect* zelfs kan leiden tot ingetoomde politieke overtuigingen en verminderde deelname aan het democratisch proces, uit angst voor represailles na kritiek op staatsinstituties.[23] Dataretentie schept theoretisch de mogelijkheid om te traceren welke personen aan bepaalde demonstraties en/of vergaderingen hebben deelgenomen. Op dat moment is een

[20] BVerfGE 65, 1, 15 december 1983
[21] Bundesverfassungsgericht 11 maart 2008, 1 BVR 256/08, par. 122-123.
[22] Ibid.
[23] Breyer 2005, p. 371.

inbreuk op de vrijheid van vergadering en vereniging aan de orde, zoals vastgelegd in artikel 11 lid 1 EVRM.[24]

De wet zal ook tot zelfcensuur van burgers aanleiding geven. Er mag niet worden voorbijgegaan aan het vage gevoel gecontroleerd te worden dat de wet kan veroorzaken, een bepalende invloed kan hebben op de uitoefening door de Europese burgers van hun vrijheid op meningsuiting en informatie, en zo een inmenging betekent op artikel 11 van het Handvest (beschouwing 52 advocaat-generaal). De rechtspraak is niet ongevoelig gebleven voor deze zogenoemde „chilling effect" doctrine (afschrikkende werking) (US Supreme Court, Wiemann/Updegraff, 344 US 183 (1952); EHRM, arrest van 25 oktober 2011, *Altuğ Taner Akçam/Turquie*, klacht nr. 27520/07, § 81; zie met name „The Chilling Effect in Constitutional Law", *Columbia Law Review*, 1969, deel 69, nr.5, blz. 808).

Het Roemeens Grondwettelijk Hof dat zich boog over de grondwettelijkheid van de Roemeense omzettingswet oordeelde hierover:[25]

> "*the regulation of a positive obligation that foresees the continuous limitation of the privacy right and the secrecy of correspondence makes the essence of the right disappear by removing the safeguards regarding its execution. The physical and legal persons, mass users of the public electronic communication services or networks, <u>are permanent subjects to this intrusion into their exercise of their private rights to correspondence and freedom of expression, without the possibility of a free, uncensored manifestation, except for direct communications</u>, thus excluding the main communication means used nowadays*". (eigen onderlijning)

Eigen vertaling:
"de regeling die een positieve verplichting oplegt die er op neer komt dat er een permanente beperking is van het recht op privacy en correspondentie maakt dat de essentie van het recht verdwijnt wanneer de veiligheidsgaranties die de uitvoering ervan vergezellen, verdwijnen. De fysische en rechtspersonen, de massagebruikers van de publieke elektronische communicatiediensten of van de netwerken, zijn permanente subjecten van deze inmenging in hun uitoefening van hun persoonlijke rechten op briefwisseling en vrije meningsuiting, wanneer de mogelijkheid niet meer bestaat tot een vrije en ongecensureerde manifestatie, met uitzondering van de directe persoon tot persoon communicatie, door de doorsnee communicatiemiddelen die vandaag courant zijn, hiervan uit te sluiten."

In zoverre bestreden wet een algehele bewaarplicht invoert schendt deze op indirecte wijze de vrije uiting van expressie en ideeën.

Het middel is gegrond.

[24] Breyer, P., Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, *European Law Journal*, Vol. 11, No. 3, May 2005, pp. 365-375.
[25] Roemenië, Grondwettelijk Hof, 8 oktober 2009, no.1258.

Tweede onderdeel

Samenvatting van het middelonderdeel

Bijhorende kosten van databewaring leiden tot minder gratis aangeboden diensten en dus een daling in de hoeveelheid data die mensen vrij zullen kunnen circuleren en schendt zodoende de vrijheid om een mening te uiten.

87.

Beperkingen op de expressievrijheid zijn onderhevig aan artikel 10, § 2 EVRM, hetwelke bepaalt:

> "*Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en 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 rechterlijke macht te waarborgen.*" *(eigen onderlijning)*

Hierin schuilt een proportionaliteiteis: de bewaarplicht zal niet verder mogen gaan dan datgene dat strikt noodzakelijk is om aan de eisen van de ingeroepen dwingende reden tegemoet komen. De inperking van de expressievrijheid zal niet verder mogen gaan dan die inperkingen die werkelijk nodig zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.

Het Roemeense Grondwettelijk Hof meent dat een aanhoudende databewaarplicht, die geen rekening houdt met de noodzakelijkheid ervan eens het doel die deze rechtvaardigde ophoudt te bestaan, het proportionaliteitsprincipe, inherent eigen aan grondrechtbeperkingen, schendt:[26]

> "*the intrusion into the free exercise of the right takes place continuously and independently of the occurrence of a justifying fact, of a determinant cause and only for the scope of criminal prevention and discovery – after their perpetration – of serious crimes*".

Eigen vertaling:
"de inmenging in de vrije uitoefening van dat recht heeft permanent plaats en onafhankelijk van een rechtvaardiging ertoe, of van een welbepaalde zaak en enkel vanuit de scope van het voorkomen van criminaliteit en van ontdekking – nadat het plaatsgreep – van ernstige misdrijven."

[26] Roemenië, Grondwettelijk Hof, 8 oktober 2009, no.1258.

Deze mogelijke beperking belet niet dat elk overheidsingrijpen op de expressievrijheid minimaal en tijdelijk moet zijn.

De overheid kiest er evenwel voor de kosten van de aanbieders voor de inzameling, registratie, bewaring en vernietiging van de gegevens, op grond van bestreden wet, niet te compenseren. Uit de memorie van toelichting bij bestreden wet blijkt dat de kosten voor de opslag als relatief klein worden beschouwd in verhouding tot alle kosten waaraan de aanbieders worden blootgesteld in het kader van de identificatie en wettelijke onderschepping. Ook de technologische vooruitgang wordt hierbij als een bijkomende reden aangestipt om een daling van de te maken kosten te verwachten.[27]

88.

De wetgever verwijst in de memorie van toelichting eveneens naar het KB van 9 januari 2003 houdende de nadere regels voor de wettelijke medewerkingsplicht dat bij gerechtelijke vorderingen met betrekking tot elektronische communicatie vergoedingen per vordering voorziet op grond van artikel 46bis en artikel 88bis van het Wetboek van Strafvordering.[28] Voormeld KB beoogt de mededeling aan de gerechtelijke autoriteiten van zowel de gegevens die worden bewaard krachtens bestreden wet als de gegevens die niet worden bewaard krachtens deze wetgeving. Voormelde vergoedingen volstaan als compensatie voor de aanbieders van bepaalde kosten inzake de opzoeking van gegevens en mededeling ervan aan de gerechtelijke autoriteiten.[29]

Eenzelfde compensatieregeling werd voorzien in het KB van 12 oktober 2010 houdende de nadere regels voor de wettelijke medewerkingsplicht bij vorderingen door de inlichtingen- en veiligheidsdiensten (artikel 7).[30]

De wetgever steunt deze beslissing op het evaluatieverslag betreffende Richtlijn 2006/24/EG inzake gegevensbewaring, dat vermeldt: "*de vergoeding van de kosten die exploitanten moeten maken als gevolg van de verplichting om gegevens te bewaren, wordt niet door de richtlijn geregeld*." En verder "*alle lidstaten kennen een of andere vorm van vergoeding indien de gegevens worden opgevraagd in het kader van een strafprocedure."*[31]

Het kostenargument is echter manifest onjuist. Uit de standpunttekst van de Belgische Internet Service Providers Association (ISPA) blijkt dat de kosten voor het verzamelen en bewaren van de gegevens substantieel hoger liggen dan de vergoedingen die nu worden voorzien (nieuwe opslagsystemen, upgrades, technische- en personeelskosten…). Voor providers die slechts enkele vorderingen ontvangen ligt de kost in verhouding zelfs hoger dan voor grote ISP's die een proportioneel aantal vorderingen ontvangen. Voor kleinere aanbieders betekent dit mogelijks de doodsteek (bestreden wet maakt immers geen onderscheid tussen de aanbieders volgens hun omvang). Het aantal diensten die gebruikers ter beschikking hebben voor het voeren van communicatie kan hierdoor slinken. Of kleine aanbieders zullen de gemaakte kosten doorrekenen

[27] Memorie van Toelichting DOC 53 29214/001, blz. 4.
[28] KB van 9 januari 2003
[29] Memorie van Toelichting DOC 53 29214/001, blz. 4 - 5.
[30] KB van 12 oktober 2010; Memorie van Toelichting DOC 53 29214/001, blz. 5.
[31] Evaluatieverslag betreffende Richtlijn 2006/24/EG inzake gegevensbewaring, nr. COM (2011) 225 p. 31.

aan hun klanten waarddoor het gebruik van communicatiemiddelen steeds duurder wordt, en dat terwijl recente mediaberichtgeving reeds gewag maakt van te duurdere telecom-prijzen in België. Vrij communiceren via telefonie- en internetdiensten moet voor iedere gebruiker een haalbare kaart blijven.[32]

89.

Bestreden wet wordt disproportioneel bevonden. De vrije uitwisseling van informatie is van het allergrootste belang in een democratische samenleving. De bewaring van verkeersgegevens heeft het effect dat communicatiestromen naar believen kunnen worden herzien. Zulks heeft een afschrikkend effect voor zowel leveranciers als ontvangers om gevoelige informatie te verspreiden. In het bijzonder maatschappijkritische informatie valt hieronder.

Bestreden wet bevat geen enkele proportionaliteitseis, noch onderwerpt zij deze beperking op de expressievrijheid aan het subsidiariteitsbeginsel (de plicht tot het kiezen van de voor de expressievrijheid minst schadelijke beperking).

Het niet compenseren van bijhorende kosten van databewaring leidt tot minder gratis aangeboden diensten en dus tot een daling in de hoeveelheid data die mensen vrij zullen kunnen circuleren. De beperking van de vrije circulatie van gedachtes en opinies beperkt aldus onrechtmatig en op onevenredige wijze de vrijheid van meningsuiting zoals beschermd door artikel 10 EVRM.

Het middel is gegrond.

Derde onderdeel

Samenvatting van het middelonderdeel

Databewaring weerhoudt providers en ontvangers van het delen van gevoelige informatie en schendt zodoende het bronnengeheim en beroepsgeheim van vertrouwensberoepen zoals advocaten, journalisten en geneesheren.

90.

Artikel 25 van de G.W. 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.*"

[32] ISPA, Position Paper Data Retention, November 2012, p. 2-3.

Het journalistiek bronnengeheim vormt één van de hoekstenen van de persvrijheid.[33] Het bronnengeheim waarborgt het recht van journalisten, en zelfs van iedereen die journalistieke activiteiten uitoefent, op geheimhouding van hun informatiebronnen.

Daarnaast wordt uitdrukkelijk de vrijheid van meningsuiting gestipuleerd in artikel 19 GGW:
"*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*."

In sommige beroepstakken geldt bovendien een beroepsgeheim. Dat betekent dat personen met bepaalde functies niets mogen bekendmaken van wat hen in hun functie werd verteld.

Een algemene bewaarplicht verstoort het beroepsgeheim van artsen, advocaten, journalisten en geestelijken, evenals politieke en zakelijke activiteiten die vertrouwelijkheid vereisen. Zonder de garantie op privacy zullen mensen minder snel geneigd zijn om met hun problemen een beroep te doen op vertrouwenspersonen.

Een enquête die werd uitgevoerd onder de bevolking in Duitsland in mei 2008 door het onderzoeksbureau Forsa heeft de nefaste gevolgen van de bewaarplicht sinds de introductie ervan in Duitsland reeds aangetoond. 52% van de ondervraagden gaf hierbij aan niet langer telefoon of e-mail te gebruiken bij vertrouwelijke contacten en 11% van de ondervraagden zou zelfs hoegenaamd geen telecommunicatie meer gebruiken.[34] Ook informanten van journalisten zullen bij een algemene bewaarplicht aarzelen om gevoelige informatie door te spelen via telecommunicatie.[35]

91.

Het beroepsgeheim en het bronnengeheim zijn nochtans fundamentele en grondwettelijk beschermde rechten die van zeer groot belang zijn bij het vrijwaren van een democratische rechtstaat. Daaruit vloeit voort dat een inbreuk op deze rechten enkel aanvaardbaar is in zeer uitzonderlijke omstandigheden, wanneer noodzaak en hoogdringendheid kunnen worden aangetoond en indien er strenge procedurele waarborgen worden gevolgd.

Zo oordeelde uw Hof in een arrest van 23 januari 2008 dat "*de strijd tegen witwaspraktijken en het financieren van terrorisme onder geen enkel beding een onconditionele en onbeperkte inbreuk op het beroepsgeheim kan rechtvaardigen*".[36]

[33] Wet van 7 april 2005 tot bescherming van de journalistieke bronnen.
[34] Kreativrauschen, Data Retention Effectively Changes the Behavior of Citizens in Germany, 4 juni 2008: http://www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/; Arbeitskreis Vorratsdatenspeicherung, Civil liberties campaigners: Communications Data Retention will be stopped, 30 juni 2008: http://www.vorratsdatenspeicherung.de/content/view/236/1/lag/en.
[35] Deutsche Telekom verdacht van afluisteren journalisten', De Standaard, 24 mei 2008, http://www.standaard.be/Artikel/Detail.aspx?artikelId=DMF24052008_046 en BRAUCK, M., ROSENBACH, M. en VERBEET, M., 'Big Brother Eyes German Journalists', Der Spiegel, 11 januari 2007: http://www.spiegel.de/international/germany/0,1518,514872-2,00.html.
[36] Grondwettelijk Hof Nr: 10/2008, 23 januari 2008, www.const-court.be.

Eisers zijn van mening dat deze waarschuwing van uw Hof geïnterpreteerd kan worden als een algemene afwijzing van disproportionele inbreuken op het beroepsgeheim en het bronnengeheim.

Ook al bestond er in 2005, in het licht van de elektronische communicatiewet, een politiek akkoord over de wijze waarop politie en justitie in welbepaalde gevallen gegevens kon opvragen van telecomoperatoren en internetproviders wil dit niet zeggen dat dit automatisch ook opgaat voor onze huidige samenleving waarbij onze wijze van communicatie sterk veranderd is en het gebruik van telecommunicatie steeds meer centraal is komen te staan. Het gevaar op een schending van de privacy evolueert uiteraard mee.

De vraag is wat de gevolgen zullen zijn voor een samenleving die niet meer buiten telecommunicatie kan, zelfs voor discrete en vertrouwelijke zaken, wanneer dit voortaan allemaal in kaart wordt gebracht. Kan een democratische samenleving zoals wij die momenteel kennen overleven wanneer het telecommunicatiegeheim op dergelijke schaal wordt prijsgegeven?

92.

Met betrekking tot de impact van de databewaringsplicht op het beroepsgeheim van bepaalde beroepsgroepen, uitte ook de Orde van Vlaamse Balies haar ongerustheid in een standpunttekst van 2009:[37]

"*Een verplichte databewaring verstoort ernstig het beroepsgeheim van de advocaat. Dit fundamenteel aspect van het beroep van advocaat is ter bescherming van de positie van de cliënt die als rechtszoekende een advocaat consulteert. Een schending hiervan wordt in ons rechtsbestel strafrechtelijk gesanctioneerd. Het is van essentieel en absoluut belang dat tussen advocaat en cliënt deze vertrouwensrelatie tot stand kan komen, ongeacht de wijze van communicatie tussen beiden (p.1).*"

Ook de Orde van Geneesheren en de journalistenvereniging VVJ/AVBB sloten zich in 2009 om bovenvermelde reden aan bij het verzetsplatform Bewaar je privacy.[38]

In zoverre een algehele bewaarplicht tot gevolg heeft dat zowel providers als ontvangers zich weerhouden van het delen van gevoelige informatie en het beroeps- en bronnengeheim van vertrouwelijke beroepsgroepen aantast, zij het dan indirect, schendt bestreden wet alle in het middel aangehaalde referentienormen.

Het middel is gegrond.

[37] Orde van Vlaamse Balies, Standpunt – Een kritische reflectie van de Europese databewaringsrichtlijn, 26 oktober 2009.
[38] www.bewaarjeprivacy.be

Derde middel

Artikel 6 en 13 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden
Artikel 14 van het Internationaal Verdrag inzake Burgerrechten en Politieke rechten
Artikel 10 en 11 van de Gecoördineerde Grondwet
Het algemeen rechtsbeginsel van het vermoeden van onschuld

GESCHONDEN REFERENTIENORMEN – Het recht op gelijke behandeling en non-discriminatie, al dan niet in samenhang met het beginsel van het vermoeden van onschuld. Het recht op een daadwerkelijk rechtsmiddel.

1. Aangevochten beschikkingen van de bestreden wet

93.

Zie eerste middel, punt 40.
Dit wordt hier voor herhaald aanzien.

2. Het onderzoekskader

94.

Zie eerste middel, punt 41-43.
Dit wordt hier voor herhaald aanzien.

3. Grieven

Eerste onderdeel

Schending van het vermoeden van onschuld

95.

De Grondwettelijke beginselen van gelijkheid en non-discriminatie (artikel 10 en 11 GGW) waarborgen de gelijke behandeling van eenieder en het genot van alle rechten en vrijheden zonder onderscheid.

Het vermoeden van onschuld is een rechtstreeks uitvloeisel en een essentieel aspect van het algemeen beginsel van het recht van verdediging.

Artikel 6. 2 EVRM omschrijft het beginsel als volgt:

"*eenieder, die wegens een strafbaar feit wordt vervolgd, wordt voor onschuldig gehouden totdat zijn schuld volgens de wet bewezen wordt*".

Het vermoeden van onschuld wordt aangetast door verklaringen of beslissingen die iemands schuld insinueren, die het publiek aansporen te geloven in iemands schuld of die vooruitlopen op de beoordeling van de feiten door de bevoegde rechter.

96.

De bewaarplicht uit bestreden wet heeft een *omkering van het vermoeden van onschuld* tot gevolg. Waar de bewijslast normaal ligt bij wie beschuldigt, moet de verdachte hier zijn onschuld bewijzen. Een categorie van burgers, met name telefoon- en internetgebruikers, bevindt zich op die manier in een manifest ongunstigere positie dan een andere, zijnde gebruikers van niet elektronische briefwisseling.

Een algemene bewaarplicht draait deze logica om en vertrekt van de idee dat elke burger potentieel gevaarlijk is. Iedere telefoon-en internetgebruiker wordt op die manier immers als een potentiële verdachte aan het preventieve toezicht van de overheid onderworpen, ook al is er geen direct noodzakelijke aanleiding.

Het is bovendien niet ondenkbaar dat iemand die voornemens is een strafbaar feit, zoals bedoeld in bestreden wet, te plegen, mogelijke mededaders of medeplichtigen hiervan per brief op de hoogte brengt. Potentiële daders zullen trachten onopgemerkt te blijven, wat meteen de vraag doet rijzen of de bewaarplicht wel zinvol is voor het doel dat zij tracht te verwezenlijken.

Aangenomen wordt dat Webmail-diensten (zoals g-mail en hotmail) niet als een elektronische communicatiedienst worden gekwalificeerd zodat deze niet onder de algehele bewaarplicht vallen.
Dat communiecatiepatronen die via deze diensten verlopen niet moeten worden bewaard kan in het licht van de nagestreefde doelstelling van bestreden wet, met name ‘vervolging van strafbare feiten, niet gerechtvaardigd worden. Er wordt bij dergelijke onderscheid van uit gegaan dat verdachte patronen zich niet via de Webmail diensten zullen openbaren. Dit verschil in behandeling kan niet worden verantwoord.

Er wordt ook voorbij gegaan aan de mogelijkheid dat iemand anders dan de eigenlijke gebruiker gebruik maakt van de telecommunicatiediensten of dat men het slachtoffer wordt van een identiteitsdiefstal, waardoor mogelijks verdachte communicatiepatronen niet in hoofde van de eigenlijke gebruiker van de dienst tot stand worden gebracht. Het zal niet zelden voorkomen dat de gebruiker niet met de bewaarde gegevens kan worden geïdentificeerd, bv. wanneer gebeld wordt met gestolen gsm’s of prepaid gsm’s. Of het internetverkeer dat door de abonnee van een internet provider wordt veroorzaakt kan niet altijd worden gekoppeld aan de persoon die daadwerkelijk gebruik heeft gemaakt van de internetverbinding, bv. internetcafés of draadloze wifi-netwerken. Daarnaast bestaan nog tal van andere mogelijkheden zoals het draaien van een eigen server, anonieme proxies, freenet, ed. In dergelijke gevallen zullen burgers geconfronteerd worden met een omkering van de bewijslast. Zij zullen immers de moeilijke taak toebedeeld krijgen om het aldus verkregen bewijsmateriaal te weerleggen.

Bestreden wet installeert als het ware een vermoeden van schuld ten laste van de telefoon- en internetgebruiker terwijl een dergelijk vermoeden niet bestaat in hoofde van gebruikers van traditionele, niet elektronische, briewisseling. Voor de ongelijke behandeling van telefoon- en internetgebruikers en gebruikers van traditionele briefwisseling, bestaat geen redelijke en objectieve verantwoording.

97.

Uw Hof ontwikkelde deze rechtspraak o.a. in arrest 81/2003 van 11 juni 2003 hetwelk bepaalt:

> "*B.5. Wettelijke vermoedens zijn in beginsel niet in strijd met die verdragsbepalingen [6.2. EVRM en 14.2. IVBPR] (EHRM, Salabiaku t/ Frankrijk, 7 oktober 1988, vol. A141-A, §28, Telfner t/ Oostenrijk, 20 maart 2001, §16).*
>
> *Zij moeten evenwel een redelijk verband van evenredigheid vertonen met het wettig nagestreefde doel (EHRM, Janosevic t/ Zweden, 23 juli 2002, §101, EHRM, Vulic t/ Zweden, 23 juli 2002, 113). Indien de wetgever aan een wettelijk vermoeden een onweerlegbaar karakter verleent, zou hij aan de essentie zelf van het vermoeden van onschuld afbreuk doen en derhalve op discriminerende wijze inbreuk plegen op voormelde verdragsbepalingen.*"[39]

Tweede onderdeel

Het ontbreken van een daadwerkelijk rechtsmiddel

98.

In artikel 13 EVRM wordt een ieder wiens rechten en vrijheden uit het verdrag worden geschonden, het recht op een daadwerkelijk rechtsmiddel voor een nationale instantie gegarandeerd, ook wanneer de schending plaatsvindt door personen in een ambtelijke functie.

Het geheime karakter van de bewaring en opvraging van de communicatie- en identificatiegegevens voorzien in de bestreden wet maakt dat het niet steeds geweten is dat een inbreuk op een grondrecht heeft plaatsgevonden, waartegen een adequaat rechtsmiddel kan aangewend worden.

Ook indien artikel 8 EVRM voldoende waarborgen voorziet, is op basis van artikel 13 EVRM een analyse nodig om uit te maken of er een nationaal wettenarsenaal aanwezig is op grond waarvan de burger zich kan verzekeren van een wetmatige toepassing van artikel 8 EVRM.

Deze vereiste is des te belangrijker wanneer het, zoals de algehele bewaarplicht uit bestreden wet, een geheime surveillance betreft.

[39] Grondwettelijk Hof, arrest van 81/2003 van 11 juni 2003.

Het individu zal weinig voordeel ondervinden van beschikbare rechtsmiddelen, wanneer de surveillance onaangekondigd, en dus buiten diens medeweten, plaatsvindt.

De hier bestreden wet voorziet geen specifiek eigen rechtsmiddel in de context van de algemene dataretentie. De burger moet teruggrijpen naar de beperkte rechtsmiddelen die in de wet op de elektronische communicatie van 13 juni 2005 en in de wet op de bescherming van de persoonlijke levenssfeer van 8 december 1992 voorzien zijn. Deze rechtsmiddelen zijn niet afdoende waar het een algemene bewaring betreft van persoonsgegevens, en het niet gaat om specifieke bewaringen zoals in beide wetten als uitgangspunt is aanvaard.

Uit jurisprudentie van het Europese Hof voor de Rechten van de Mens blijkt dat onder omstandigheden een kennisgevingsplicht een geëigende invulling is van de eis die uit artikel 13 EVRM voortvloeit, te weten dat een ieder die meent dat ten aanzien van hem artikel 8 van het EVRM is geschonden, recht heeft op een daadwerkelijk rechtsmiddel voor een nationale instantie.

Bij voorkeur moet met een zo groot mogelijke mate van precisie worden aangegeven in het belang van welke doelstellingen uitstel van de kennisgevingsplicht is toegestaan en wordt niet volstaan met een ruime uitzonderingscategorie zoals "noodzakelijk in een democratische samenleving".

Immers op grond van artikel 8 EVRM dient iedere beperking in zijn totaliteit reeds aan die voorwaarde te voldoen. Deze jurisprudentie laat wel uitzonderingen op de onverwijlde kennisgevingsplicht toe in het belang van de strafvordering en de nationale veiligheid.

Het Europees Hof oordeelde hierover in *Klass*[40] dat het ontbreken van bovenvermelde kennisgeving geen schending uitmaakt van artikel 13, wanneer een voldoende aantal kwalitatieve alternatieven aanwezig is.

Gezien geen daadwerkelijk rechtsmiddel wordt voorzien, zou kunnen aangenomen worden dat bestreden wet een onweerlegbaar vermoeden instelt. Bovendien lijkt door de wetgever de noodzakelijkheid en proportionaliteit van de bewaarplicht niet bewezen. Het naar voren geschoven cijfermateriaal en de willekeurige voorbeelden die werden aangehaald in de bijlage van de Memorie van Toelichting bij het voorontwerp van wet van 27 augustus 2009 voldeden hiertoe niet. Indien de noodzaak van een algehele bewaarplicht niet kan worden aangetoond, zal het daarmee gepaard gaande wettelijke vermoeden ook buiten proportie zijn.

99.

Algemeen wordt aangenomen dat een ongelimiteerde toegang tot de bewaarde persoonsgegevens, op elk mogelijk tijdstip, moeilijk als gerechtvaardigd en noodzakelijk, alsook proportioneel in functie van het nagestreefde doel kan worden beschouwd.

Ook het Europees Hof voor de Rechten van de Mens deed uitspraak over het vermoeden van onschuld in het Marper arrest.[41]

[40] Klass t Duitsland, App. 5029/71, 6 september 1978, Series A, No 28 51979-80° 2 EHRM 214

Het Hof wees op het risico van stigmatisering, door het onbeperkt opslaan van persoonlijke gegevens, volgend uit het feit dat personen zoals S en Marper, die niet waren veroordeeld voor enig misdrijf en derhalve recht hadden op de presumptie van onschuld, werden behandeld op dezelfde wijze als veroordeelde personen. De perceptie dat zij niet werden behandeld als onschuldige personen werd naar het oordeel van het Hof vergroot door het feit dat hun data voor onbepaalde tijd werden bewaard op dezelfde wijze als de data van veroordeelde personen:

> "*122. Of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons. […]*
> *It is true that the retention of the applicants' private data cannot be equated with the voicing of suspicions. Nonetheless, their perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed."*

Eigen vertaling:
"122. Een bijzondere bezorgdheid in deze context is het risico op stigmatisering, uitgaand van het feit dat personen in de situatie van verzoekers, die nooit veroordeeld zijn voor een misdrijf en die zich kunnen beroepen op het vermoeden van onschuld, op dezelfde wijze behandeld worden als personen die veroordeeld zijn. …
Het is juist dat het bewaren van de private data van verzoekers niet kan gerechtvaardigd worden door zich te beroepen op verdenkingen. Desalniettemin, hun perceptie dat zij niet behandeld worden als onschuldig is in hoge mate ook ernstig doordat hun data voor onbeperkte tijd bewaard worden zoals bij veroordeelde personen, terwijl de data van zij die nooit verdacht werden van een misdrijf wel vernietigd worden."

Ook de Orde van Vlaamse Balies wijst in haar standpunttekst van 2009 op de verregaande implicaties die deze massale opslag van gegevens met zich meebrengt, o.a. voor het vermoeden van onschuld:[42]
"*Bovendien druist het idee dat elke burger potentieel gevaarlijk is in tegen het vermoeden van onschuld dat een fundamenteel recht is in ons rechtsbestel. De Orde benadrukt dat iedereen wordt geacht onschuldig te zijn, tot zijn schuld volgens de wet bewezen wordt (p.1).*"
Om die reden eist de Orde van Vlaamse Balies dat voor elke raadpleging van de bovenvermelde gegevens een onafhankelijke rechter toeziet op mogelijke inbreuken op de bovenvermelde fundamentele rechten van de burger. Enkel de onderzoeksrechter die als onpartijdige en onafhankelijke rechter op zoek gaat naar zowel belastend als ontlastend bewijsmateriaal, mag de toelating om de gegevens te raadplegen, geven (p.2).
In zoverre bestreden wet een systematische en voortdurende bewaarplicht voorstaat van alle elektronische telecommunicatiegegevens, ongeacht hiervoor een direct noodzakelijke aanleiding bestaat, waardoor burgers in hun fundamenteel vermoeden van onschuld worden aangetast, schendt deze alle in het middel aangehaalde referentienormen.

---

[41] EHRM S. en Marper t Verenigd Koninkrijk, 4 december 2008.
[42] Orde van Vlaamse Balies, Standpunt – Een kritische reflectie van de Europese databewaringsrichtlijn, 26 oktober 2009.

Met betrekking tot dit vermoeden van onschuld oordeelde het Roemeense Grondwettelijk Hof[43] tot de onrechtmatigheid van de inbreuk op het recht op privacy niet enkel omwille van de mogelijkheid tot identificatie van de zender van de boodschap, maar ook van de ontvanger hiervan.

Deze laatste wordt blootgesteld aan de opslag van mogelijks gevoelige persoonsgegevens, buiten zijn eigen wil of gedragingen, maar op de basis van het gedrag van anderen. Ondanks zijn "passieve" rol in de communicatie, kan de ontvanger verdacht worden in hoofde van de overheidsdiensten die belast zijn met strafrechtelijk onderzoek. Ook vanuit dit opzicht is de bewaarplicht buitensporig:

> *"this operation equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes".*

100.

De bestreden wet, m.n. het preventief registreren van eenieders verkeers- en locatiegegevens, leidt er toe dat er definitief afstand wordt gedaan van het principe dat mensen als onschuldig behandelt tot het tegendeel is bewezen.

Hierdoor komen we terecht in een samenleving die haar eigen burgers wantrouwt in plaats van ze te beschermen. Het beweerde bestaan van een terreurdreiging is geen vrijgeleide om de fundamentele beginselen van de rechtstaat buitenspel te zetten. Communicatiebeginselen zijn immers veel meer dan een eenvoudige weergave van wie met wie wanneer belt. Verkeersgegevens worden nu gebruikt om associaties tussen mensen in kaart te brengen en, belangrijker nog, om activiteiten en voornemens van mensen af te leiden.

Wanneer men dit in de bredere context plaatst van de stijgende tendens om enorme nationale databanken op te richten met interoperationaliteit op Europees niveau en een uitgebreide toegang voor politionele doeleinden, wordt een algemene bewaarplicht van telecommunicatiegegevens des te beangstigender. Gegevens die oorspronkelijk enkel verzameld werden voor de vereisten van een bepaalde dienstverlening worden dan ingezet voor het toezicht op burgers en sociale controle, en in het ergste geval voor inlichtingsdoeleinden. Deze maatregel is dan ook een zoveelste uiting van een 'cultuur van controle' die de laatste decennia in onze West-Europese samenleving steeds meer genormaliseerd wordt en die in algemene zin meer gericht is op uitsluiting dan op solidariteit, meer op sociale controle dan op sociale voorzieningen, en meer op particuliere vrijheid van de markt dan op publieke vrijheden van universeel burgerschap.

Het middel is gegrond.

[43] Roemenië, Grondwettelijk Hof, 8 oktober 2009, no.1258.

Vierde middel

Artikel 1 van het 1e protocol bij het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden;
Artikel 10, 11, 16 van de Gecoördineerde Grondwet;
Het algemeen rechtsbeginsel van proportionaliteit;
Artikel 1 PECHR;

GESCHONDEN REFERENTIENORMEN – Recht op eigendom, al dan niet in samenhang gelezen met het algemeen rechtsbeginsel van proportionaliteit

1. Aangevochten beschikkingen van de bestreden wet

101.

Zie eerste middel, punt 40.
Dit wordt hier voor herhaald aanzien.

2. Het onderzoekskader

102.

Zie eerste middel, punt 41-43.
Dit wordt hier voor herhaald aanzien.

3. Grieven

Eerste onderdeel

Samenvatting van het middelonderdeel
Databewaring weerhoudt providers van een doeltreffend genot van hun eigendom

103.

De rechtspraak van het EHRM aanvaardt dat het klantenbestand van een bedrijf wordt beschermd als eigendom onder artikel 1 PECHR. Een wettelijke verplichting die aldus leidt tot een verlies aan klanten voor bedrijven schendt het recht op eigendom. Dataretentie wordt als wettelijke verplichting aan alle aanbieders van telecommunicatie opgelegd, zonder onderscheid, en zou in deze dus geen nadelig effect hebben voor individuele bedrijven in het bijzonder. Inzonderheid voor kleine ISP's is de bewaarplicht een loodzware opdracht, en zullen zij trachten om deze niet

of niet consequent toe te passen. Ook in het buitenland gevestigde providers en telecommaatschappijen, en dan inzonderheid in landen (ook binnen de EU) die geen dataretentiewetgeving hebben, moeten zich niet aan deze verplichting, die belangrijke financiële consequenties heeft, houden, met een evident concurrentieel voordeel.

In dit opzicht plaatsen kleinere ISP's en buitenlandse ISP's zich dus in een concurrentieel voordeel ten aanzien van de grote en in België opererende ISP's die de bewaarplicht niet kunnen omzeilen, daar de eersten zich kunnen onttrekken aan de aanzienlijke kost die daarmee gepaard gaat en zij bovendien aantrekkelijke aanbieders worden ten aanzien van klanten die een provider verkiezen die hun communicatiegegevens niet opslaat.[44]

Op die wijze schendt de wet het eigendomsrecht.

Tweede onderdeel

Samenvatting van het middelonderdeel

Databewaring bepaalt het gebruik dat providers van hun eigendom maken

104.

Een ongewilde ontneming van eigendom door de staat valt binnen het wettelijk toepassingsgebied van artikel 1, 1ste lid PECHR indien dit dezelfde effecten ressorteert als formele onteigening. Dit is het geval wanneer het genot van het recht op eigendom niet kan plaatsvinden op enige doelgerichte manier, als een gevolg van de maatregel. Een dergelijke maatregel kan enkel proportioneel worden geacht indien de wet voorziet in een passende compensatie.

De toestellen en servers die ISP's gebruiken voor het aanbieden van hun diensten vallen onder de bescherming van het recht op eigendom uit artikel 1 PECHR. Een algehele bewaarplicht schendt de aanbieders in dit eigendomsrecht wanneer de apparaten die voorheen werden gebruikt voor de dienstverlening, niet verder kunnen worden gemoderniseerd om de kost van dataretentie mogelijk te maken. Dergelijke apparaten worden, als een gevolg hiervan, onbruikbaar en verliezen aldus hun waarde. Om die reden vereist artikel 1, 2de lid PECHR een adequate vergoeding voor bedrijven die met dergelijke financiële verliezen te maken krijgen.

Een algehele bewaarplicht dwingt de ISP's tot een bepaald gebruik van hun eigendom, teneinde in overeenstemming te zijn met de wettelijke verplichting. Vermoedelijk zullen bepaalde apparaten uitsluitend gebruikt worden voor de opslag van data, zonder nog enig ander doel te dienen. De bestreden wet bepaalt aldus het gebruik dat ISP's van hun eigendom maken en vormt zodoende een inbreuk op artikel 1 PECHR.

[44] Breyer, P., Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, *European Law Journal*, Vol. 11, No. 3, May 2005, p. 374-375.

De inbreuk kan, op grond van artikel 1, 2de lid PECHR, enkel gerechtvaardigd worden in het kader van het algemeen belang. In dit opzicht wordt een ruime appreciatiemarge aan de lidstaten gegeven, zij het dat de inbreuk steeds proportioneel dient te zijn.

Inzake dataretentie is reeds voldoende uit de cijfers gebleken dat deze maatregel weinig doeltreffend is maar wel een zware financiële last legt op de ISP's die er onderhevig aan zijn.

Het gebrek aan financiële compensatie is een disproportionele aantasting van het recht op eigendom

OM DEZE REDENEN
En alle andere in te roepen terloops het geding, eventueel ambtshalve,
BEHAGE HET UW GRONDWETTELIJK HOF,

Het beroep tot vernietiging ontvankelijk en gegrond te verklaren;

In hoofdorde,

Dienvolgens, de artikels 1, 2, 3, 4, 5, 6 en 7 van de wet van 30 juli 2013 tot wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van strafvordering (bekendgemaakt in het Belgisch Staatsblad van 23 augustus 2013) te vernietigen;

In ondergeschikte orde,

Vooraleer recht te doen volgende prejudiciële vragen te stellen aan het Europees Hof van Justitie te Luxemburg.

1. Is de richtlijn en zijn inzonderheid de artikelen 3 tot en met 9 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 en tot wijziging van richtlijn 2002/58/EG, verenigbaar met de artikelen 7, 8 en 11 van het Handvest en/of met artikel 8 en 10 EVRM?

2. Moeten, gelet op de toelichting bij artikel 8 van het Handvest, die overeenkomstig artikel 52, lid 7, daarbij is opgesteld om richting te geven aan de uitlegging van dit Handvest, 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 verordening

(EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens [PB 2001, L 8, blz. 1], bij de beoordeling van de toelaatbaarheid van inmengingen in aanmerking worden genomen op dezelfde voet als de voorwaarden van artikel 8, lid 2, en artikel 52, lid 1, van het Handvest?

3. Hoe verhoudt het in artikel 52, lid 3, laatste zin, van het Handvest genoemde 'recht van de Unie' zich tot de richtlijnen op het gebied van het recht inzake gegevensbescherming?

4. Moet, gelet op het feit dat richtlijn 95/46/EG en verordening (EG) nr. 45/2001 voorwaarden en beperkingen stellen aan de uitoefening van het in het Handvest neergelegde fundamentele recht op gegevensbescherming, bij de uitlegging van artikel 8 van het Handvest rekening worden gehouden met wijzigingen ten gevolge van afgeleid recht van latere datum?

5. Heeft, gelet op artikel 52, lid 4, van het Handvest, het in artikel 53 van het Handvest neergelegde beginsel van voorrang van het hogere beschermingsniveau tot gevolg dat de in het Handvest neergelegde grenzen voor de toelaatbare beperkingen door afgeleid recht nauwer moeten worden afgebakend?

6. Kunnen, gelet op artikel 52, lid 3, van het Handvest, de vijfde alinea van de preambule en de toelichting op artikel 7 van het Handvest, volgens welke de in artikel 7 gewaarborgde rechten corresponderen met de rechten die in artikel 8 EVRM zijn gewaarborgd, aan de rechtspraak van het Europees Hof voor de Rechten van de Mens inzake artikel 8 EVRM criteria worden ontleend voor de uitlegging van artikel 8 van het Handvest, die de uitlegging van laatstgenoemd artikel beïnvloeden?"

7. Is de beperking van de rechten van verzoekers welke voortvloeit uit de vereisten van de artikelen 3, 4 en 6 van richtlijn 2006/24/EG, onverenigbaar met artikel 5, lid 4, VEU, voor zover zij onevenredig is en niet noodzakelijk of niet geschikt is om de volgende legitieme doelen te bereiken: a) het mogelijk maken dat bepaalde gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige strafbare feiten? en/of b) het waarborgen van de goede werking van de interne markt van de Europese Unie?

8. In hoeverre vereisen de verdragen – en in het bijzonder het in artikel 4, lid 3, VEU vervatte beginsel van loyale samenwerking – dat een nationale rechterlijke instantie onderzoekt en beoordeelt of de nationale maatregelen ter uitvoering van richtlijn 2006/24/EG verenigbaar zijn met de bescherming die wordt geboden door het Handvest, waaronder artikel 7 daarvan (zoals geïnspireerd door artikel 8 EVRM)?"

Onder voorbehoud van alle rechten en zonder enige nadelige erkentenis, noch verzaking.

Brussel, 23 februari 2014

Voor verzoekers, hun raadsman,

Raf JESPERS

Inventaris van de stukken

1. Bestreden wet
2. Bekendmaking statuten eerste verzoekster
3. Beslissing van eerste verzoekster tot het instellen van het beroep en mandaat aan advocaat voor procedure
4. Bekendmaking statuten tweede verzoekster
5. Beslissing van tweede verzoekster tot het instellen van het beroep en mandaat aan advocaat voor procedure
6. Advies advocaat-generaal dd. 12 december 2013 Europees Hof van Justitie zaken C-293/12 en C-594/12.