VERZOEKSCHRIFT INHOUDEND HET BEROEP TOT VERNIETIGING

van de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten (bekendgemaakt in het Belgisch Staatsblad van 8 augustus 2022)

Aan de Dames en Heren Voorzitters en Rechters van het Grondwettelijk Hof van België.

Geachte Dames en Heren,

Geeft U met eerbied te kennen :

V.Z.W. LIGA VOOR MENSENRECHTEN ingeschreven in de kruispuntbank voor ondernemingen onder het ondernemingsnummer 0419.191.537, met zetel te 1080 Sint-Jans-Molenbeek, Leopold II Laan 53,

Verzoeker,
met als raadsman Mr Raf Jespers

Verzoeker kiest woonst bij zijn advocaat meester Raf Jespers, advocaat te

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 stelt verzoeker hierbij beroep in strekkend tot de vernietiging van de **artikelen 1 tot en met 48 van de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten (bekendgemaakt in het Belgisch Staatsblad van 8 augustus 2022);**

Verzoeker voegt 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 (stuk 1).

INHOUDSTAFEL

I. Voorwerp van de procedure p.3
I.1. Vernietiging artikels 1 tot en met 48 Dataretentiewet van 20 juli 2022 p.3
I.2. Context van het verzoekschrift p.3

II. Ontvankelijkheid van het beroep p.4
II.1. Belang p.4
II.2. De termijnen p.6

III. Toepasselijke Wettelijke en Verdragsrechtelijke Bepalingen p.6
III.1. Het Unierecht p.6
III.2. EVRM en Grondwet p.7

IV. Procedures Hof van Justitie en Grondwettelijke Hoven p.8
IV.1. Procedures HvJ met betrekking tot artikel 15.1 Richtlijn 2002/58/EG p.8
IV.2. Procedure La Quadrature du Net p.9
IV.3. Arresten HvJ Commissioner en SpaceNet p.12
IV.4. Procedures Grondwettelijke Hoven EU p. 12
IV.5. Procedures Belgisch Grondwettelijk Hof p.13

V. Advies Belgische Gegevensbeschermings Autoriteit (GBA) p. 15

VI. De Middelen p.21
VI.1. Eerste middel: wet voert een algemene en ongedifferentieerde bewaring van gegevens in, en een toegang tot de gegevens buiten het kader van de doelstellingen van artikel 15.1 e-Privacy Richtlijn 2002/58/EG p. 23
VI.2. Tweede middel: de door de operatoren te bewaren gegevens beantwoorden wat hun aantal en categorieën betreft niet aan de voorwaarden van proportionaliteit en noodzakelijkheid p. 35
VI.3. Derde middel: de bewaring van gegevens in geografische zones voert *de iure* en *de facto* een algemene en ongedifferentieerde opslag van gegevens in p. 61
VI.4. Vierde middel: de wettelijke regeling verleent toegang tot de bewaarde gegevens aan autoriteiten die niet onder de doelstellingen van artikel 15.1 e-Privacy Richtlijn 2002/58/EG vallen. Bovendien zijn de voorwaarden voor toegang niet in overeenstemming met vermeld artikel en met de rechtspraak HvJ p. 92
VI.5. Vijfde middel: de wettelijke regeling maakt geen differentiëring wat betreft de gegevens die beschermd zijn door het beroepsgeheim van advocaten, artsen en journalisten p. 100

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

I.1. Vernietiging van de artikels 1 tot en met 48 van de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten

1. Verzoeker stelt een beroep tot vernietiging in van de artikels 1 tot en met 48 van de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten (bekendgemaakt in het Belgisch Staatsblad van 8 augustus 2022). Deze wet wordt als stuk gevoegd bij dit verzoekschrift. De bestreden artikels van de wet worden onder de middelen weergegeven.

   De bestreden artikels van de wet van 20 juli 2022 worden in de middelen opgenomen met verwijzing naar de artikels die opgenomen en/of gewijzigd werden in de wet van 13 juni 2005 betreffende elektronische communicatie, inhoudend de bepalingen van de gegevens die door de operatoren verplicht moeten bewaard worden. Er wordt in het middel aangeduid door welk artikel van de wet van 20 juli 2022 de artikels in de wet van 13 juni 2005 werden ingevoerd.

2. Niet alle artikels van de wet van 20 juli 2022 zijn in de middelen als te vernietigen opgenomen. Wegens het ondeelbaar karakter van die artikels met de te vernietigen artikels, dient de wet in haar geheel te worden vernietigd. (Zie overweging B.12. arrest 84/2015 GwH van 11 juni 2015, waarbij de dataretentiewet van 30 juli 2013 vernietigd werd; zie overweging B.20. arrest 57/2021 GwH van 22 april 2021, waarbij de dataretentiewet van 29 mei 2016 vernietigd werd).

I.2. Context van het verzoekschrift

3. Verzoeker wijst er op dat de huidige betwisting de zogenaamde derde Belgische dataretentiewet betreft. De eerste en tweede datarentietwet werden door uw Hof vernietigd. De tweede dataretentiewet werd door uw Hof vernietigd na het stellen van prejudiciële vragen aan het Hof van Justitie van de Europese Unie (HvJ). Uw Hof volgde in haar arrest over de tweede dataretentiewet het standpunt van het HvJ.

   In dit kader verwijst verzoeker naar uw overwegingen B.18 en B.19 in het arrest GwH nr. 57/2021 van 22 april 2021 waarbij de tweede dataretentiewet werd vernietigd. Deze overwegingen worden verder integraal geciteerd. Deze overwegingen stellen dat de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie ‘de uitzondering moet zijn, en niet de regel’ en de regeling ‘de inmenging tot het strikt noodzakelijke moet beperken’ en ‘moet beantwoorden aan objectieve criteria’. Verder wordt gesteld dat een regeling ‘in het licht van de rechtspraak van het Hof van Justitie en in voorkomend geval met de door dat Hof aangebrachte preciseringen’ tot stand dient gebracht te worden.

   Het arrest GwH van 22 april 2021 verwijst naar het arrest HvJ La Quadrature du net van 6 oktober 2020, waarbij ook verzoeker voor België betrokken partij was. Inmiddels heeft het HvJ haar standpunt

van La Quadrature de Net bevestigd in de arresten Commissioner of An Garda Siochana (C-140/20, 5 april 2022) en SpaceNet AG (C-156/22 van 20 september 2022).

4. Verzoeker is van mening dat de derde datarentiewet in tegenstelling tot wat vermelde rechtspraak vooropstelt, van de inmenging niet de uitzondering maar opnieuw de regel maakt en op het vlak van bewaring van gegevens en toegang tot de gegevens, integendeel de inmenging nog uitgebreider maakt dan in de eerste en tweede dataretentiewet. Dit zal in de middelen duidelijk ontwikkeld worden. Indicatief is de enorme uitbreiding in de hier bestreden wet van de diverse door de operatoren te bewaren gegevens. Indicatief is in de hier bestreden wet dat de toegang tot de bewaarde gegevens (onder diverse modaliteiten) wordt toegestaan aan tien onderscheiden autoriteiten terwijl dit in de eerste dataretentiewet ging om vier autoriteiten en in de tweede dataretentiewet om acht autoriteiten.

5. De Belgische Gegevensbeschermingsautoriteit (GBA) heeft uitgebreid standpunt ingenomen over het voorontwerp op basis waarvan de hier bestreden wet tot stand kwam. Tussen het voorontwerp en de wet zelf zijn geen wezenlijke verschillen. Het standpunt van de GBA wordt verder opgenomen. De GBA stelt dat het voorontwerp van wet 'niet echt de perspectiefwijzing inhoudt als vereist door de jurisprudentie van het HvJ en het Grondwettelijk Hof' en dat het 'van cruciaal belang is ervoor te zorgen dat het voorontwerp van wet niet *de jure* of *de facto* opnieuw een veralgemeende en ongedifferentieerde verplichting invoert om de verkeers- en locatiegegevens te bewaren van alle of een te groot deel van de gebruikers van elektronische communicatie in België.'

II. Ontvankelijkheid van het beroep

II.1. Met betrekking tot het belang

6. Voor een vereniging zonder winstoogmerk (VZW), die voor het Hof optreedt, is het een vereiste dat zij een maatschappelijk doel van bijzondere aard heeft, onderscheiden van het algemeen belang; dat zij een collectief belang verdedigt; dat haar maatschappelijk doel door de bestreden wet kan worden aangetast.

7. Verzoeker: VZW Liga voor Mensenrechten

Artikel 3 en 4 van haar statuten luiden:

"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 3)

"*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 van vergaderingen, het tussenkomen bij de overheden, het indienen van klachten bij de gerechtelijke overheden en het instellen van rechtsgedingen*. " (artikel 4)

Het maatschappelijk doel van verzoeker is bijgevolg van bijzondere aard en onderscheiden van het algemeen belang.

8. De bestreden wet (hierna : Dataretentiewet van 20 juli 2022) voert wijzigingen in van de wet van 13 juni 2005 betreffende de elektronische communicatie.

   De aangevochten wet is van aard om allerlei grondrechten aan te tasten, zoals 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 recht op een eerlijk proces, het recht op een daadwerkelijk rechtsmiddel, alsook het wettigheidsbeginsel in strafzaken, het proportionaliteitsbeginsel, het rechtszekerheidsbeginsel, het evenredigheidsbeginsel en het beginsel van het vermoeden van onschuld.

   Verzoeker steunt het beroep tot vernietiging op de schending van vermelde grondrechten, die gewaarborgd worden 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, 11, 12, 14, 15, 17 en 19 van het Internationaal Verdrag inzake Burgerrechten en Politieke rechten goedgekeurd bij wet van 15 mei 1981 (hierna: IVBPR);
- artikel 15, lid 1 van de richtlijn 2002/58/EG zoals gewijzigd bij richtlijn 2009/136 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);
- artikel 23, lid 1 van de Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van

persoonsgegevens en betreffende het vrij verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming);
- artikelen 12, 13,14,19, 22, 25, 26 en 27 van de Gecoördineerde Grondwet (hierna: G.W.);
- artikel 544 Burgerlijk Wetboek

Het maatschappelijk doel van verzoeker – de bescherming van vermelde grondrechten – kan door de aangevochten wet en de toekomstige uitspraak in het gedrang komen, zodat zijn belang in deze procedure vaststaat.

Uw Grondwettelijk Hof aanvaardde trouwens het vereiste belang van verzoeker in tal van arresten o.a. : GwH 22 april 2021, nr. 57/2021; GwH 11 juni 2015, nr. 84/2015; 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.

II.2. Met betrekking tot de termijnen

9. Het beroep tot vernietiging van de bestreden wet is ingesteld binnen de zes maanden na de bekendmaking ervan.

III. Toepasselijke wettelijke en verdragsrechtelijke bepalingen

III.1. Het Unierecht: de Richtlijn betreffende privacy en elektronische communicatie 2002/58/EG en de Verordening (EU) 2016/679 van het Europees Parlement.

10. **Richtlijn 2002/58/EG** *"betreffende privacy en elektronische communicatie"* (hierna: ePrivacy-richtlijn) is een specificatie voor de telecommunicatiesector van het algemene juridische regime voor gegevensbescherming, vervat in richtlijn 95/46/EG. (zie EHJ, arrest Tele2 Sverige AB van 21 december 2016, 82).

Het gaat in wezen om een beschermingsrichtlijn.

Artikel 15 van de ePrivacy-richtlijn geeft de lidstaten de bevoegdheid om uitzonderingen vast te stellen op o.a. artikel 6 van de ePrivacy-richtlijn, In verband met belangen verband houdend met de rechtshandhaving. De lidstaten zijn daarbij gebonden aan het Unierecht. Artikel 15 lid 1 noemt in het bijzonder artikel 6 lid 1 en 2 van het Unieverdrag, en bindt de lidstaten daarmee uitdrukkelijk aan fundamentele rechtsbeginselen.

Artikel 15.1:

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

11. **Richtlijn 2016/680** van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad. Artikel 15 en 54 van deze Richtlijn bepalen respectievelijk welke informatie de verantwoordelijke voor de behandeling van gegevens moet verschaffen aan de betrokkene, en het recht op effectief juridisch verweer in geval de voorziene informatie niet wordt gegeven.

III.2. Artikel 8 EVRM, artikel 10, 11 en 22 Grondwet, artikel 7, 8, 11 en 52.1 Handvest Grondrechten Europese Unie

12. Hierna vermelde arresten van het Hof van Justitie en van de Grondwettelijke Hoven nemen artikel 7 en 8 Handvest als toetsingskader in nauw verband met artikel 8 EVRM en de rechtspraak van het EHRM (zie bijvoorbeeld verwijzingen in overwegingen 35, 54 en 55 van het arrest van 8 april 2014 van het HvJ).

Artikel 7 Handvest:

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

Artikel 8 Handvest:

'Eenieder heeft recht op de bescherming van zijn persoonsgegevens. 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. Een onafhankelijke autoriteit ziet er op toe dat deze regels worden nageleefd.'

Artikel 8 EVRM:

‘Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. 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.’.

Het recht op privacy (artikel 7 van het Handvest, vergelijkbaar met artikel 8 van het EVRM) en het recht op gegevensbescherming (artikel 8 van het Handvest) zijn als afzonderlijke grondrechten in het Handvest opgenomen, maar staan wel nadrukkelijk met elkaar in verband. Artikel 7 wordt doorgaans eerder beschouwd als een klassiek grondrecht dat beschermt tegen inbreuk, terwijl artikel 8 meer de grondwettelijke spelregels uitstippelt voor de gegevensbescherming.

Ook artikel 11.1 (‘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.’) en 52.1 van het Handvest formuleren betrokken rechten (‘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 achtname 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’) zijn betrokken rechten.

Voor België verwijst verzoeker naar Grondwetsartikel 10 (‘Er is in de Staat geen onderscheid van standen. De Belgen zijn gelijk voor de wet. …’), 11 (‘Het genot van de rechten en vrijheden aan de Belgen toegekend moet zonder discriminatie verzekerd worden. Te dien einde waarborgen de wet en het decreet inzonderheid de rechten en vrijheden van de ideologische en filosofische minderheden.’) en 22 (‘Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaalt.’)

IV. Procedures en rechtspraak Hof van Justitie EU en Grondwettelijke Hoven

IV.1. Procedures voor het Europees Hof van Justitie (HvJ) in verband met Richtlijn 2002/58/EG en artikel 15.1 van de Richtlijn

13. Het Digital Rights arrest van 8 april 2014 (C-293/12 en C-594/12) verklaarde de Dataretentie Richtlijn 2006/24/EG van 15 maart 2006, ongeldig. Het HvJ oordeelde dat de bewaring a priori, veralgemeend en onbepaald van metadata een ongeoorloofde inmenging is.

Na het DRI-arrest zijn bij het HvJ twee zaken aanhangig gemaakt over de in Zweden en in het Verenigd Koninkrijk aan de aanbieders van elektronische communicatiediensten opgelegde algemene verplichting tot bewaring van de gegevens betreffende deze communicaties, welke bewaring door de

ongeldig verklaarde richtlijn was voorgeschreven. De dag na het arrest Digital Rights Ireland heeft het telecommunicatiebedrijf Tele2 Sverige de Zweedse toezichthoudende autoriteit voor post en telecommunicatie officieel laten weten dat het had beslist, de gegevens niet meer te bewaren, en van plan was, de tot dan toe bewaarde gegevens te vernietigen. Het Zweedse recht verplichte de aanbieders van elektronische communicatiediensten immers alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronische communicatiemiddelen stelselmatig en voortdurend te bewaren en voorziet niet in enige uitzondering.

14. Na de vernietiging van de Dataretentierichtlijn, verschoof de discussie bij het HvJ naar de toepassing van de e-Privacy Richtlijn 2002/58/EG en inzonderheid artikel 15.1 van die Richtlijn.

In het Tele 2 Sverige arrest van 21 december 2016 (C-203/15) oordeelde het HvJ dat artikel 15.1 van de e-Privacy Richtlijn zich verzet tegen een nationale regeling die, te bestrijding van criminaliteit, voorziet in een algemene en ongedifferentieerde bewaring van alle verkeersgegevens. Verder werd gesteld dat de toegang tot gegevens alleen kan ter bestrijding van ernstige criminaliteit, moet toegang onderworpen aan voorafgaand toezicht door rechterlijke instantie of onafhankelijke bestuurlijke autoriteit en mits verplichting de gegevens te bewaren op het grondgebied van de Unie.
In dit arrest wordt al gesteld dat bewaring en toegang twee onderscheiden inmengingen zijn, en aan aparte criteria moeten beantwoorden.

IV.2. Procedure in verband met Richtlijn 2002/58/EG inzake de prejudiciële vragen van het Belgisch Grondwettelijk Hof. Het arrest La Quadrature du Net van 6 oktober 2020

15. Naar aanleiding van het verzoek tot nietigverklaring ingesteld tegen de tweede Belgische dataretentiewet van 29 mei 2016, heeft het Belgische Grondwettelijk Hof bij een tussenarrest van 19 juli 2018 prejudiciële vragen gesteld aan het Hof van Justitie inzake de toepassing van artikel 15, lid 1 van Richtlijn 2002/58/EG.

In het arrest van 6 oktober 2020 (zaken C 511/18, C 512/18 en C 520/18; arrest La Quadrature du Net en anderen onder meer huidige verzoeker) heet het HvJ zich alsvolgt uitgesproken (beschikkend gedeelte):

Het Hof (Grote kamer) verklaart voor recht:

1) Artikel 15, lid 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), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in die bepaling genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring

van verkeers- en locatiegegevens. Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, verzet zich daarentegen niet tegen wettelijke maatregelen

– die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische communicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;
– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;
– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;
– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen, en
– die het mogelijk maken om ten behoeve van de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronische communicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode,

mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik.

2) Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, moet aldus worden uitgelegd dat het zich niet verzet tegen een nationale regeling die aanbieders van elektronische communicatiediensten verplicht om, ten eerste, met name verkeers- en locatiegegevens op geautomatiseerde wijze te analyseren en in real time op te vragen, en, ten

tweede, technische gegevens over de locatie van de gebruikte eindapparatuur in real time op te vragen, wanneer

- die geautomatiseerde analyse beperkt is tot situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en de toepassing van die analyse effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of er sprake is van een situatie die de genoemde maatregel rechtvaardigt en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer
- het in real time opvragen van verkeers- en locatiegegevens beperkt is tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten, en is onderworpen aan voorafgaande toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, om ervoor te zorgen dat een dergelijke maatregel slechts wordt toegestaan binnen de grenzen van het strikt noodzakelijke. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden.

3) Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt („richtlijn inzake elektronische handel") moet aldus worden uitgelegd dat zij niet van toepassing is op de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij. Deze bescherming wordt, naargelang van het geval, beheerst door richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, of door verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming). Artikel 23, lid 1, van verordening 2016/679, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd.

4) Een nationale rechterlijke instantie mag geen bepaling van haar nationale recht toepassen die haar machtigt om de werking in de tijd te beperken van de door haar op grond van dit recht uit te spreken onwettig verklaring van een nationale wettelijke regeling waarbij ten behoeve van met name de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronische communicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten. Op grond van artikel 15, lid 1, uitgelegd in het licht van het

doeltreffendheidsbeginsel, dient de nationale strafrechter informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten.

IV.3. De arresten HvJ Commissioner van 5 april 2022 (C-140/20) of An Garda Siochana en SpaceNet AG (C-793/19 en C-794/19) van 20 september 2022

16. In deze arresten heeft het HvJ in grote lijnen het standpunt van La Quadrature du Net bevestigd. Verzoeker zal deze arresten aanwenden en citeren onder de middelen.

    Het betrof eveneens prejudiciële vragen. Het arrest SpaceNet AG oordeelde over de Duitse dataretentie wet TKG.

IV.4. Procedures voor de Grondwettelijke Hoven in de EU

17. In een aantal lidstaten werd nationale datawetgeving als ongrondwettig beschouwd.

    Het Duitse Bundesverfassungsgericht vernietigde al een aantal jaren voor het Digital Rights-arrest van het HvJ de Duitse wetgeving inzake dataretentie. (Bundesverfassungsgericht, arrest van 2 maart 2010, nr. 256/08, 263/08 en 586/08. Zie over dit arrest meer uitgebreid: E. de Vries, R. Bellanova, P. de Hert en S. Gutwirth, "The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)", in S. Gutwirth, Y. Poullet, P. de Hert en R. Leenes (eds.), Computers, privacy and data protection: an element of choice, Springer, 2011, 3-24.)

    Na de ongeldigverklaring van de Dataretentierichtlijn volgde het Verfassungsgerichtshof van Oostenrijk (Oostenrijks Verfassungsgerichtshof, arrest G 47/2012 van 27 juni 2014.)

    Ook een aantal Grondwettelijke Hoven in de EU volgden daarna het Duitse en Oostenrijkse voorbeeld. Zo bijvoorbeeld Slovakije (schorsingsarrest van 23 april 2014); Slovenië (uitspraak van 3 juli 2014); Roemenië (uitspraak van 8 juli 2014); Bulgarije (uitspraak van 12 maart 2015).

IV.5. Procedures voor het Belgisch Grondwettelijk Hof

18. De huidige procedure betreft de derde Dataretentiewet. De twee vorige wetten werden door het Belgisch Grondwettelijk Hof vernietigd:

Arrest GwH nr. 84/2015 van 11 juni 2015 vernietigt de wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90 decies van het Wetboek van strafvordering. Het GwH geeft volgend motief:

> B.11. Om dezelfde redenen als die welke het Hof van Justitie van de Europese Unie ertoe hebben gebracht de « Dataretentierichtlijn » ongeldig te verklaren, dient te worden vastgesteld dat de wetgever, met de aanneming van artikel 5 van de bestreden wet, de grenzen heeft overschreden die worden opgelegd door de eerbiediging van het evenredigheidsbeginsel in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie. Het voormelde artikel 5 schendt bijgevolg de artikelen 10 en 11 van de Grondwet, in samenhang gelezen met die bepalingen. Het enige middel in de zaak nr. 5856 en het eerste middel in de zaak nr. 5859 zijn gegrond.
>
> B.12. Wegens hun ondeelbaar karakter met artikel 5, dienen ook de artikelen 1 tot 4, 6 en 7 van de bestreden wet van 30 juli 2013, en dus de wet in haar geheel, te worden vernietigd.

Tussenarrest GwH nr. 96/2018 van 19 juli 2018 waarbij prejudiciële vragen worden gesteld aan het Hof van Justitie van de Europese Unie.

Arrest GwH nr. 57/2021 van 22 april 2021vernietigt de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en bewaren van de gegevens in de sector van de elektronische communicatie. Het GwH sluit zich aan bij de antwoorden van het HvJ op de prejudiciële vragen.

Het GwH geeft volgende motivering:

> B.15. Uit het voormelde arrest van het Hof van Justitie van 6 oktober 2020 in zake La Quadrature du Net e.a., blijkt dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus moet worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in dat artikel 15, § 1, genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, behalve in de in het voormelde arrest beschreven beperkte gevallen. In zoverre zij principieel en zonder beperking tot die gevallen voorziet in een algemene en ongedifferentieerde bewaring, door de operatoren en aanbieders van elektronische communicatiediensten, van de identificatiegegevens, de toegangs- en verbindingsgegevens, alsook van de communicatiegegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, schendt de bestreden wet bijgevolg artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de voormelde bepalingen van het Handvest van de grondrechten van de Europese Unie, en in samenhang met de artikelen 10 en 11 van de Grondwet.
>
> B.16.1. In het dictum van het voormelde arrest van 6 oktober 2020, in zake La Quadrature du Net e.a., preciseert het Hof van Justitie echter dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen

in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, zich niet verzet tegen verschillende soorten wettelijke maatregelen die het Hof opsomt. Toelaatbaar zijn aldus, met name, wettelijke maatregelen « die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk », of nog wettelijke maatregelen « die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen ». Die wettelijke maatregelen moeten, « door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik ».

B.16.2. Op grond van die preciseringen van het Hof van Justitie betoogt de Ministerraad in zijn aanvullende memories dat de bestreden wet in elk geval niet dient te worden vernietigd in zoverre zij voorziet in de algemene en ongedifferentieerde verplichting tot bewaring, door de operatoren en aanbieders van elektronische communicatiediensten, van de IP-adressen die zijn toegewezen aan de bron van een verbinding, enerzijds, en van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen, anderzijds. De Ministerraad besluit daaruit dat, in voorkomend geval, enkel het tweede en het derde lid van artikel 126, § 3, van de wet van 13 juni 2005 dienen te worden vernietigd, waarin respectievelijk de verbindings- en locatiegegevens en de communicatiegegevens worden beoogd. Hij is van mening dat het eerste lid van het voormelde artikel 126, § 3, waarin de identificatiegegevens worden beoogd, daarentegen niet dient te worden vernietigd, net zomin als de andere bepalingen van de bestreden wet, aangezien zij de nodige waarborgen bevatten op het vlak van bewaring van en toegang tot de gegevens.

B.17. Te dezen dient te worden vastgesteld dat de bestreden wet, wat het beginsel zelf ervan betreft, berust op een verplichting tot algemene en ongedifferentieerde bewaring van alle gegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, en dat zij, in het algemeen, zoals in B.3 en B.4 is vermeld, ruimere doelstellingen nastreeft dan de bestrijding van zware criminaliteit of het risico van aantasting van de openbare veiligheid. Het onderscheid dat bij artikel 126, § 3, van de wet van 13 juni 2005 wordt gemaakt tussen drie categorieën van gegevens (te weten : identificatiegegevens, toegangs- en verbindingsgegevens, alsook communicatiegegevens) heeft slechts een weerslag op het startpunt van de bewaringstermijn van de gegevens - in elk geval twaalf maanden -, en eventueel op de mogelijkheden voor de gemachtigde instanties om toegang tot die gegevens te hebben (zie artikel 46bis van het Wetboek van strafvordering en artikel 126, §2, van de wet van 13 juni 2005). Die categorisering stemt daarenboven niet overeen met het onderscheid dat door het Hof van Justitie in zijn arrest van 6 oktober 2020 wordt gemaakt voor wat betreft de verschillende categorieën van gegevens die het voorwerp kunnen uitmaken van een verplichting tot algemene en ongedifferentieerde bewaring, mits verscheidene voorwaarden in acht worden genomen (te weten, te dezen : de IP-adressen die zijn toegewezen aan de bron van een verbinding

en de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen).

B.18. Bij het arrest van het Hof van Justitie van 6 oktober 2020 wordt een verandering van gezichtspunt opgelegd ten opzichte van de keuze die de wetgever heeft gemaakt : de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel. De regeling waarbij in een dergelijke verplichting wordt voorzien, moet daarenboven onderworpen zijn aan duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd (punt 133). Die regeling moet waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt en moet steeds « beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel » (punten 132 en 133).

B.19. Het staat aan de wetgever een regeling tot stand te brengen waarbij de beginselen in acht worden genomen die van toepassing zijn inzake bescherming van persoonsgegevens, in het licht van de rechtspraak van het Hof van Justitie, en, in voorkomend geval, rekening te houden met de door dat Hof aangebrachte preciseringen wat betreft de verschillende soorten wettelijke maatregelen die verenigbaar worden geacht met artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie. In het bijzonder staat het, in die context, ook aan de wetgever tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat, voor elk soort gegeven, de inmenging tot het strikt noodzakelijke wordt beperkt.

B.20. Rekening houdend met hetgeen voorafgaat, dienen de artikelen 2, b), 3 tot 11 en 14 van de bestreden wet, die onlosmakelijk met elkaar verbonden zijn, te worden vernietigd.

V. Het advies van de Belgische Gegevensbeschermingsautoriteit (GBA) met betrekking tot het voorontwerp van de hier bestreden wet 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten.

19. De GBA gaf advies nr. 108/2021 van 28 juni 2021.

De GBA stelt (vet door GBA):

OM DIE REDENEN,

Oordeelt de Autoriteit dat de volgende aanpassingen moeten worden aangebracht in het voorontwerp van wet en in het ontwerpbesluit:

- De noodzaak en evenredigheid van de verplichting tot bewaring van de locatie- en andere verkeersgegevens nodig voor het opsporen en analyseren van een vermoed geval van fraude of een vermoed geval van kwaadwillig gebruik van het elektronisch communicatienetwerk onderwerpen aan een strikte analyse en het ontwerp in die zin aanpassen en/of de relevante rechtvaardiging opnemen in de memorie van toelichting (punt 67-69)

-Indien de wetgever na die analyse meent dat het strikt noodzakelijk en evenredig is om een verplichting tot bewaring van de verkeersgegevens op te leggen voor de bestrijding van fraude en kwaadwillig gebruik van het netwerk, moeten de volgende aanpassingen worden aangebracht:

➢ De precieze gegevens bepalen die moeten worden bewaard in toepassing van die verplichting of de Koning verplichten om die gegevens te bepalen (punt72)

➢ Preciseren dat de mogelijkheid om de gegevens na de minimumtermijn van 4 maanden te bewaren betrekking heeft op situaties waarin een langere bewaartijd nodig is om een geschil betreffende fraude of kwaadwillig gebruik van het netwerk te beheren (punt 73)

-De noodzaak en evenredigheid van de verplichting tot bewaring van de locatie- en andere verkeersgegevens nodig om de veiligheid en de correcte werking van de netwerken en diensten voor elektronische communicatie te garanderen onderwerpen aan een strikte analyse en het ontwerp in die zin aanpassen en/of de relevante rechtvaardiging opnemen in de memorie van toelichting (punt 78-80)

-Indien de wetgever na die analyse meent dat het strikt noodzakelijk en evenredig is om een verplichting tot bewaring van de verkeersgegevens op te leggen om de veiligheid en de correcte werking van de netwerken en diensten voor elektronische communicatie te garanderen, moeten de volgende aanpassingen worden aangebracht:

➢ De precieze gegevens bepalen die moeten worden bewaard in toepassing van die verplichting of de Koning verplichten om die gegevens te bepalen (punt 82)

➢ Beoordelen en, in voorkomend geval, rechtvaardigen waarom een bewaarduur van 12 maanden aangewezen is (punt 83)

➢ Preciseren dat de mogelijkheid om de gegevens na de termijn van 12 maanden te bewaren betrekking heeft op situaties waarin een langere bewaarperiode nodig is om een geschil betreffende een aanslag of handelingen die de veiligheid van het netwerk of de correcte werking van de dienst in gevaar brengen te beheren (punt 83)

-Preciseren dat deze wettelijke verplichting die wordt vermeld in de artikelen 122 § 4/2 en 123 enkel kan worden opgelegd door een formele wetgevende norm (punt 85-89)

-De noodzaak en evenredigheid van de verplichting tot bewaring van de andere locatiegegevens dan verkeersgegevens voor de verschillende doelen die zijn geïdentificeerd door het nieuwe artikel 123 van de telecomwet onderwerpen aan een strikte analyse en het ontwerp in die zin aanpassen en/of de relevante rechtvaardiging opnemen in de memorie van toelichting (punt 87-88)

-In voorkomend geval ten minste de voorwaarden bepalen waaronder de operatoren de andere locatiegegevens dan verkeersgegevens mogen bewaren en verwerken, evenals de maximale bewaarduur van deze gegevens (punt 88)

-Bepalen dat de IP-adressen toegewezen aan de bron van de verbinding enkel mogen worden bewaard met het oog op bijzonder belangrijkste doelstellingen (punt 97,100)

-Verduidelijken dat alleen IP-adressen die zijn toegewezen aan de bron van een verbinding, en niet IP-adressen die zijn toegewezen aan de bestemming van een communicatie, mogen worden bewaard op grond van het nieuwe artikel 126 van de telecomwet (punt 100)

-Bepalen dat het preventief en systematisch bewaren van de identificatienummers van de eindapparaten van de eindgebruikers enkel wordt opgelegd om een doelstelling van bijzonder belang (zoals de bestrijding van zware criminaliteit) na te streven, dat de bewaarduur strikt beperkt is tot die doelstelling en de strikte voorwaarden en waarborgen bepalen voor het gebruik van die gegevens (punt 102)

-De mogelijkheid schrappen voor de operatoren om voor de identificatie van hun abonnees gebruik te maken van de gezichtsherkenningstechniek (of een andere techniek op basis van het gebruik van biometrische gegevens) (punt 104)

-De door de operator te verzamelen en te bewaren identificatiegegevens en - documenten bepalen of de Koning verplichten om die gegevens en documenten te bepalen (punt 105)

-Het begrip "communicatiegegevens" bepalen (punt 109)

-Het begrip "gegevens van oproeppogingen zonder resultaat" bepalen of die uitdrukking vervangen door de uitdrukking "verkeersgegevens van de oproeppogingen zonder resultaat" (punt 110)

-In het besluit van 19 september de woorden "ten minste" schrappen opdat dit besluit een volledige opsomming zou geven van de gegevens die de operatoren moeten bewaren in uitvoering van het nieuwe artikel 126/1 van de telecomwet (punt 113)

-Ervoor zorgen dat de drempel die wordt weerhouden om een zone aan te merken als bijzonder blootgesteld aan feiten van zware criminaliteit de facto niet kan leiden tot een verplichting tot algemene en ongedifferentieerde bewaring van de gegevens op (bijna) het hele nationale grondgebied (punt 117)

-Erop toezien dat de nadere regels om te bepalen of een zone bijzonder blootgesteld is aan feiten van zware criminaliteit passend zijn (punt 122-124)

-Erop toezien dat de keuze van plaatsen die worden weerhouden om er een gerichte preventieve bewaring van gegevens op te leggen voldoet aan de eisen van noodzaak en evenredigheid (punt 125)

-De machtiging aan de Koning om andere plaatsen toe te voegen dan deze die zijn opgesomd in het voorontwerp van wet schrappen (punt 125)

-Aanvulling van de gegevens die moeten worden opgenomen in het jaarlijks verslag dat de minister van Telecommunicatie en de minister van Justitie aan de Kamer moeten voorleggen (punt 126-127)

-Preciseren dat onder de "gegevens" de "gegevens bedoeld in §2" moet worden verstaan (punt 128)

-De mogelijkheid schrappen die de operatoren wordt geboden om gegevens te bewaren van buiten de geografische zones waarbinnen het voorontwerp van wet voorziet in een bewaarplicht wanneer het voor hen technisch niet mogelijk is om de gegevensbewaring te beperken tot die zones (punt 129-130)

-De formulering van de aanduiding van de verwerkingsverantwoordelijke aanpassen (punt 132)

-Bepalen dat alle door de operatoren bewaarde gegevens worden bewaard op het grondgebied van de Unie (punt 136)

-Bepalen dat de volgende gegevens moeten worden opgenomen in het logboek:
✓ Het concrete doel waarvoor de toegang tot de gegevens wordt gevraagd, met dien verstande dat dit doel "omfloerst" moet worden opgetekend (punt 137)
✓ Elke handeling in het logboek (punt 137)

-De reikwijdte verduidelijken van het nieuwe artikel 127/2 § 2, eerste en laatste lid (punt 139-140)

-De begrippen "aanbieders van private elektronische communicatienetwerken" en "aanbieders van elektronische communicatiediensten die niet openbaar beschikbaar zijn" definiëren (punt 143)

-Bepalen dat de autoriteiten toegang tot de in toepassing van de artikelen 122 en 123 bewaarde gegevens kunnen krijgen voor andere doeleinden dan deze waarvoor ze oorspronkelijk werden bewaard, maar alleen als die latere verwerkingsdoelen de bescherming van de nationale veiligheid of de bestrijding van zware criminaliteit betreffen (of een ander doel dat is vermeld in artikel 15 van de ePrivacyrichtlijn en eenzelfde graad van belangrijkheid heeft) (punt 152)

-De relevante bepalingen aanpassen om erop toe te zien dat de toegang tot de gegevens, conform de Europese eisen, steeds onderworpen is aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit die de hoedanigheid heeft van derde ten opzichte van de autoriteit die de toegang tot de gegevens heeft gevraagd, behalve in de gevallen van naar behoren gerechtvaardigde spoedeisendheid (punt 153-155)

-Uitdrukkelijk de opdrachten specificeren waarvoor het BIPT toegang kan krijgen tot de door de operatoren bewaarde verkeersgegevens (punt157).

-Schrapping van het verbod op het gebruik van systemen die de identificatie, tracering en plaatsbepaling van niet-openbaar beschikbare communicatie door de eindgebruiker en de bewaring van identificatie-, verkeers- of locatiegegevens kunnen verhinderen (punt 162)

-Schrapping van de verplichting voor operatoren die een versleutelingssysteem opzetten om legale interceptiemaatregelen mogelijk te maken (punt 163)

-In het besluit van 19 september 2013 de verwijzing naar 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 schrappen aangezien het HvJ-EU deze richtlijn ongeldig heeft verklaard (punt 164).

De Autoriteit vestigt de aandacht op de volgende factoren:

-De wetgeving dient na te gaan of alle bepalingen die de autoriteiten machtigen om toegang te krijgen tot de door de operatoren bewaarde verkeers- en locatiegegevens voorzien in de nodige materiële en procedurele voorwaarden om aan de Europese eisen te voldoen (punt 154)

-De rechterlijke instantie of de onafhankelijke bestuurlijke entiteit die het toezicht uitvoert dat een communicatie van de gegevens voorafgaat, moet nagaan of met die communicatie een van de toegelaten doeleinden wordt nagestreefd en of ze voldoet aan het evenredigheidsbeginsel (punt 156)

BIJLAGE I Executive Summary

De minister van Justitie, de heer Vincent Van Quickenborne, vroeg op 7 mei 2021 het advies van de Autoriteit over een voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie- , verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten (hierna "het voorontwerp van wet") en over een ontwerp van koninklijk besluit tot wijziging van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna "het ontwerp van besluit").

Het voorontwerp van wet beoogt tegemoet te komen aan de vernietiging van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie. Op 21 april 2021 vernietigde het Grondwettelijk Hof deze wet van 29 mei 2016, die in beginsel was gebaseerd op een veralgemeende en ongedifferentieerde verplichting om verkeers- en locatiegegevens van gebruikers van elektronische communicatiemiddelen te bewaren. Het Grondwettelijk Hof, waarvan de motivering grotendeels verwijst naar het arrest van het Hof van Justitie van de Europese Unie (HJEU) van 6 oktober 2020 (het " Quadrature du Net "-arrest), is evenwel van oordeel **dat de verplichting om gegevens met betrekking tot elektronische communicaties te bewaren de uitzondering moet zijn, en niet de regel.** In zijn arrest herinnert het Grondwettelijk Hof eraan dat "het aan de wetgever staat, in het licht van de rechtspraak van het Hof van Justitie een regeling uit te werken die de beginselen eerbiedigt die van toepassing zijn op de bescherming van persoonsgegevens, en in voorkomend geval rekening te houden met de verduidelijkingen die het Hof heeft aangebracht met betrekking tot de verschillende soorten wetgevingsmaatregelen die verenigbaar worden geacht met [de ePrivacyrichtlijn, gelezen in het licht van het Handvest van de grondrechten van de Europese Unie]".

Het voorontwerp van wet beoogt de invoering van een bewaarsysteem voor communicatiemetadata dat voldoet aan de eisen van het Europees recht, zoals geïnterpreteerd door het HvJEU (voor een overzicht van dit systeem, zie de tabel in Bijlage II). **Er zij echter op gewezen dat het voorontwerp van wet niet echt de perspectiefwijziging inhoudt als vereist door de jurisprudentie van het HvJEU en het Grondwettelijk Hof.** In haar advies merkt de Autoriteit op dat het voorontwerp van wet voornemens is nieuwe maatregelen voor de bewaring van verkeers- en locatiegegevens op te leggen, hetgeen zou kunnen leiden tot de feitelijke herinvoering van veralgemeende en ongedifferentieerde verplichtingen inzake gegevensbewaring, terwijl tegelijkertijd de mogelijkheden voor toegang tot dergelijke gegevens worden uitgebreid. **Het is waar dat de bewaring van metagegevens noodzakelijk kan zijn om het recht op veiligheid van personen te waarborgen, dat evenals het recht op bescherming van de persoonlijke levenssfeer en van persoonsgegevens een grondrecht is dat is verankerd in de Belgische Grondwet, het Europees Verdrag tot bescherming van de rechten van de mens en het Handvest van de grondrechten van de Europese Unie.** Het recht op veiligheid schept positieve verplichtingen voor de staat om materiële en procedurele maatregelen te nemen om strafbare feiten tegen personen doeltreffend te bestrijden door middel van doeltreffende opsporing en vervolging. Het HvJEU erkent de noodzaak om deze verschillende grondrechten met elkaar te verzoenen. **De Autoriteit verzoekt de wetgever de tijd te nemen om na te denken en grondig te analyseren hoe, overeenkomstig de Europese jurisprudentie, het grondrecht op veiligheid en het recht op een doeltreffende voorziening in rechte in geval van strafbare feiten die deze veiligheid aantasten, enerzijds, en het grondrecht op eerbiediging van het privéleven en op bescherming van persoonsgegevens, anderzijds, met elkaar kunnen worden verzoend.** De Autoriteit dringt er bij de wetgever op aan het voorontwerp van wet aan te passen om ervoor te zorgen dat de aan te nemen wet voldoet aan alle door het HJEU en het Grondwettelijk Hof opgelegde vereisten. Een nieuwe nietigverklaring van de wet door het Grondwettelijk Hof zou het vertrouwen van de burgers in de democratische instellingen waarschijnlijk ondermijnen. **Het is daarom van cruciaal belang ervoor te zorgen dat het voorontwerp van wet niet *de jure of de facto* opnieuw een veralgemeende en ongedifferentieerde verplichting invoert om de verkeers- of locatiegegevens te bewaren van alle of een te groot deel van de gebruikers van elektronische communicatie in België.** In haar advies heeft de Autoriteit een groot aantal opmerkingen over het voorontwerp van wet, waarin wordt gewezen op de aanpassingen die moeten worden aangebracht om te waarborgen dat de ontwerpregeling voldoet aan de vereisten van het recht op bescherming van persoonsgegevens, zoals geïnterpreteerd door het HJEU.

Voorts stelt **de Autoriteit met bezorgdheid vast dat het voorontwerp van wet voorziet in een verplichting voor operatoren die een versleutelingssysteem opzetten, om rechtmatige interceptiemaatregelen mogelijk te maken,** met name de identificatie van de eindgebruiker, het traceren en lokaliseren van niet voor het publiek toegankelijke communicatie, en het aftappen en opnemen van niet voor het publiek toegankelijke communicatie. Sinds de jaren negentig bestaat er in de wetenschappelijke gemeenschap een consensus dat het inbouwen van "achterdeurtjes" (" backdoors") in versleutelingssystemen meer risico's inhoudt voor de persoonlijke levenssfeer van de betrokken personen en voor de belangen van de staten dan dat het voordelen oplevert voor de bestrijding van zware criminaliteit. **De Autoriteit is ook bezorgd over de invoering van een gegevensverzamelingsplicht door diensten, zoals de versleutelde berichtendiensten, die tot dusver om legitieme veiligheids- en privacyredenen hebben vermeden om dergelijke gegevens te verzamelen.**

VI. De middelen

20. Logica, structuur en opbouw van de middelen

Er worden vijf middelen ontwikkeld. Het eerste middel betreft de beoordeling van de wetsschendingen door de wet van 20 juli 2022 in zijn geheel. Het tweede middel betreft de schending door de bepalingen inzake gegevens te bewaren door de operatoren. Het derde middel betreft de schending door de bepalingen inzake de gegevens te bewaren in geografische zones. Het vierde middel betreft de schending door de bepalingen die aan autoriteiten toegang verlenen tot de gegevens. Het vijfde middel betreft de schending van de wet van het beroepsgeheim van advocaten, artsen en journalisten.

Bij de beoordeling van de opgeworpen schendingen wordt in de middelen een onderscheid gemaakt tussen enerzijds het bewaren van gegevens en anderzijds de toegang tot de gegevens.

De structuur van elk middel: geschonden wetsbepalingen; aangevochten wettelijke bepalingen en systematisering ervan; standpunt Europees hof van Justitie EU (HvJ) en systematisering ervan; toepassing en discussie.

Het HvJ heeft gesteld dat zowel het bewaren als de toegang tot de gegevens onderscheiden inmengingen in de grondrechten uitmaken en een verschillende rechtvaardiging vereisen. In het arrest SpaceNet AG was aan de orde de vraag of een nationale wettelijke regeling die zorgt voor de volledige naleving van de voorwaarden die voortvloeien uit de rechtspraak inzake toegang tot de bewaarde gegevens afdoende is om de resulterende ernstige inmenging in de rechten van de betrokken personen die het gevolg is van de bewaring van de gegevens te verhelpen of beperken. Met andere woorden: volstaat een afdoende bescherming van de toegang ook als een afdoende bescherming met betrekking tot de bewaring.

“Derhalve biedt richtlijn 2002/58 **niet enkel voor de toegang tot die gegevens waarborgen tegen misbruik**, maar erkent zij met name ook het **beginsel dat die gegevens niet door derden mogen worden opgeslagen** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 39).” (HvJ, SpaceNet AG, C-793/19 en C-794/19, 20 september 2022, punt 56; HvJ, perscommuniqué nr. 156/22).

De logica van de rechtspraak van het HvJ houdt in dat wanneer de bewaring van de gegevens op zich in strijd is met de wetsbepalingen in het middel, de toegang tot de gegevens ook problematisch is daar er geen geldige toegang kan zijn tot gegevens die niet conform de wettelijke bepalingen bewaard worden. Omgekeerd is de toegang tot de gegevens die conform de wettelijke bepalingen is, geen rechtvaardiging om de bewaring van de gegevens conform de wettelijke bepalingen te aanvaarden.

21. Essentiele referentiekaders

- Het arrest van het Belgisch Grondwettelijk Hof nr. 57/2021 van 22 april 2021 waarbij de (tweede) dataretentiewet van 29 mei 2016 vernietigd werd. Dit arrest werd uitgesproken na een tussenarrest

nr. 96/2018 van 19 juli 2018, waarbij prejudiciële vragen werden gesteld aan het Hof van Justitie van de Europese Unie. Het arrest van 22 april 2021 sluit zich aan bij het arrest van het HvJ van 6 oktober 2020 (arrest La Quadrature du Net, Liga voor Mensenrechten, Ligue des droits humains…), waarbij de prejudiciële vragen werden beantwoord.

- Volgende arresten van het HvJ:

< Arrest La Quadrature du Net e.a. van 6 oktober 2020 in de zaken C-511/18, C-512/18 en C-520/18. (verder genoemd La Quadrature du Net)

< Arrest G.D. tegen Commissioner of An Garda Siochana, e.a. van 5 april 2022 in de zaak C-140/20. (verder genoemd Commissioner of An Garda Siochana)

< Arrest Bundesrepublik Deutchland tegen SpaceNet AG en Telekom Deutschland GmbH van 20 september 2022 in de zaken C-793/19 en C-794/19. (verder genoemd SpaceNet AG). Dit arrest had als voorwerp de Duitse Telekommunikationsgesetz (TKG) telecommunicatiewet van 22 juni 2004 na prejudiciële vragen ingediend door het Bundesverwaltungsgericht (hoogste federale bestuursrechter, Duitsland)

Verzoeker wijst op het belang van de recente arresten van 5 april 2022 en 20 september 2022; zij bevestigen het standpunt dat het HvJ heeft ingenomen in La Quadrature du Net en voorheen in Tele Sverige en Watson (arresten van 21 december 2016, C-203/15 en C-698/15).

Deze arresten. spreken zich, zoals het arrest La Quadrature du Net, uit over de toepassing van artikel 15, lid 1 en de artikels 5, 6 en 9 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), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

VI.1. EERSTE MIDDEL

Geschonden wetsartikels en referentienormen

Schending van artikel 11, 12, 22 en 29 Grondwet.

Schending van artikel 15, lid 1 en de artikels 5, 6 en 9 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), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

Schending van artikel 6, 8, 10, 11 en 18 van het Europees Verdrag voor de bescherming van de Rechten van de Mens (EVRM).

Schending van de artikels 13 en 54 van de Richtlijn 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Geschonden referentienormen.

Recht op eerbiediging van de persoonlijke levenssfeer en bescherming van persoonlijke data, al dan niet in samenhang gelezen met het recht op vertrouwelijkheid van communicatie en met de algemene beginselen van informatieve zelfbeschikking en de beginselen van noodzaak in een democratische samenleving, legaliteit, proportionaliteit en subsidiariteit.

Schending van de in het middel vermelde wettelijke bepalingen door de artikels 122, 123, 126, 126/1 en 126/2, 126/3 en 127/1 ingevoegd of gewijzigd door de artikels 5, 6, 8, 9, 10, 11, 12 en 13 van de wet van 20 april 2022 in de wet van 13 juni 2005 betreffende elektronische communicatie, inhoudend de bepalingen van de gegevens die de operatoren verplicht moeten bewaren, de gegevens die in de geografische zones moeten bewaard worden en de autoriteiten die toegang hebben tot de gegevens. De wet voert een algemene en ongedifferentieerde bewaring van gegevens in. De wet verleent toegang tot de gegevens aan autoriteiten die vallen buiten het kader van de doelstellingen van algemeen belang van artikel 15.1 e-Privacy Richtlijn

A. De bestreden wettelijke bepalingen

22. De bestreden wet van 20 april 2022 voert met de artikels 5, 6, 8, 9, 10, 11, 12 en 13 een geheel van maatregelen in die *de iure* en *de facto* een algemene bewaarplicht van communicatiegegevens invoert en een zeer brede toegang tot de bewaarde gegevens instelt. Vermelde artikels voeren in de wet van 13 juni 2005 betreffende de elektronische communicatie respectievelijk de artikels 122, 123, 126, 126/1, 126/2, 126/3, 127 en 127/1 in.

B. <u>Het algemene en principiële standpunt van het Hof van Justitie inzake dataretentie</u>

23. Met betrekking tot de interpretatie van artikel 15, lid 1 van richtlijn 2002/58/EG, worden in het arrest SpaceNet onder de punten 49-75 principiële overwegingen gegeven 'in het licht waarvan de door de verwijzende rechter onder de aandacht gebrachte kenmerken van de in het hoofdgeding aan de orde zijnde nationale regeling moeten worden onderzocht'. (punt 76). Punt 75 formuleert op duidelijke wijze de gevallen waarbij wettelijke maatregelen kunnen genomen worden ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen voor de openbare veiligheid. Dit punt 75 stemt grotendeels overeen met het beschikkend gedeelte van het arrest HvJ La Quadrature du Net.

Verzoeker stelt dat deze principiële overwegingen ook gelden voor de beoordeling van de hier bestreden wet van 20 juli 2022 in zijn geheel en in zijn onderdelen.

24. Toepasselijke passages uit arrest HvJ SpaceNet van 20 september 2022 in verband met toepassing artikel 15, lid 1 Richtlijn 2002/58:

Uitlegging van artikel 15, lid 1, van richtlijn 2002/58

Overzicht van de uit de rechtspraak van het Hof voortvloeiende beginselen

49 Volgens vaste rechtspraak moet bij de uitlegging van een Unierechtelijke bepaling niet alleen rekening worden gehouden met de bewoordingen van de bepaling in kwestie, maar ook met de **context van deze bepaling en met de doelstellingen** die worden nagestreefd met de regeling waarvan zij deel uitmaakt, en dient bij die uitlegging met name de **totstandkomingsgeschiedenis** van deze regeling in aanmerking te worden genomen (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 32 en aldaar aangehaalde rechtspraak).

50 Uit de bewoordingen zelf van artikel 15, lid 1, van richtlijn 2002/58 blijkt dat de wettelijke maatregelen die de lidstaten onder de in deze richtlijn gestelde voorwaarden mogen treffen, **enkel** kunnen zien op de **„beperking van de reikwijdte" van de rechten en verplichtingen die zijn neergelegd in onder meer de artikelen 5, 6 en 9 van die richtlijn** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 33).

51 Met betrekking tot het bij richtlijn 2002/58 ingevoerde stelsel, waarvan artikel 15, lid 1, deel uitmaakt, dient in herinnering te worden gebracht dat de lidstaten op grond van artikel 5, lid 1, eerste en tweede volzin, van die richtlijn door middel van hun **nationale wetgeving het vertrouwelijke karakter van de via openbare communicatienetwerken en via openbare**

elektronische-communicatiediensten tot stand gebrachte communicatie alsook van de daarmee verband houdende verkeersgegevens moeten waarborgen. Zij moeten met name het **afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van communicatie** en daarmee verband houdende verkeersgegevens door anderen dan de gebruikers **verbieden** wanneer de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat overeenkomstig artikel 15, lid 1, van richtlijn 2002/58 bij wet is toegestaan (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 34).

52 In dit verband heeft het Hof reeds geoordeeld dat artikel 5, lid 1, van richtlijn 2002/58 het beginsel van vertrouwelijkheid van zowel elektronische communicatie als de daarmee verband houdende verkeersgegevens erkent en onder meer impliceert dat het anderen dan de gebruikers **in beginsel verboden is om die communicatie en die gegevens op te slaan zonder toestemming van die gebruikers** (arresten van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 107, en 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 35).

53 Deze bepaling weerspiegelt de **doelstelling die de Uniewetgever** nastreefde toen hij richtlijn 2002/58 vaststelde. Uit de toelichting bij het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 def.], waaruit richtlijn 2002/58 is voortgekomen, blijkt namelijk dat de Uniewetgever heeft beoogd „verder te zorgen voor een **hoge mate van bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronische-communicatiediensten, ongeacht de gebruikte technologie”**. Zoals onder meer uit de overwegingen 6 en 7 van richtlijn 2002/58 volgt, heeft deze richtlijn dan ook tot doel de gebruikers van elektronische-communicatiediensten te **beschermen tegen de gevaren die de nieuwe technologieën en in het bijzonder de steeds grotere mogelijkheden tot geautomatiseerde opslag en verwerking van gegevens met zich meebrengen voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers.** Zoals in overweging 2 van die richtlijn staat te lezen, wenst de Uniewetgever met name de **volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest** neergelegde rechten te waarborgen, welke rechten betrekking hebben op de bescherming van het privéleven respectievelijk de bescherming van persoonsgegevens (zie in die zin arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 36 en aldaar aangehaalde rechtspraak).

54 Met de vaststelling van richtlijn 2002/58 heeft de Uniewetgever deze **rechten dan ook geconcretiseerd**, zodat de gebruikers van elektronische-communicatiemiddelen er in beginsel op mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet worden opgeslagen, tenzij zij met het tegendeel hebben ingestemd (arresten van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 109, en 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 37).

55 Wat betreft de verwerking en de opslag door aanbieders van elektronische-communicatiediensten van **verkeersgegevens** die betrekking hebben op abonnees en

gebruikers, bepaalt artikel 6 van richtlijn 2002/58 in lid 1 dat deze gegevens moeten worden **gewist of anoniem moeten worden gemaakt wanneer zij niet langer nodig zijn** voor het doel van de transmissie van communicatie, en preciseert dat artikel in lid 2 dat verkeersgegevens die noodzakelijk zijn ten behoeve van de facturering van abonnees en interconnectiebetalingen slechts mogen worden verwerkt tot aan het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen. Wat **andere locatiegegevens dan verkeersgegevens** betreft, bepaalt artikel 9, lid 1, van richtlijn 2002/58 dat deze gegevens slechts **onder bepaalde voorwaarden mogen worden verwerkt nadat zij anoniem zijn gemaakt** dan wel de gebruikers of abonnees daarvoor hun **toestemming** hebben gegeven.

56 Derhalve biedt richtlijn 2002/58 **niet enkel voor de toegang tot die gegevens waarborgen tegen misbruik**, maar erkent zij met name ook het **beginsel dat die gegevens niet door derden mogen worden opgeslagen** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 39).

57 Omdat de lidstaten op grond van artikel 15, lid 1, van richtlijn 2002/58 **wettelijke maatregelen mogen treffen ter „beperking van de reikwijdte"** van de in onder meer de artikelen 5, 6 en 9 van deze richtlijn neergelegde rechten en verplichtingen – zoals die welke voortvloeien uit de in punt 52 van het onderhavige arrest in herinnering gebrachte beginselen van vertrouwelijkheid van communicatie en van het verbod op het opslaan van daarmee verband houdende gegevens – vormt die bepaling **een uitzondering op de algemene regel die in onder meer die artikelen 5, 6 en 9 is neergelegd,** zodat zij volgens vaste rechtspraak **restrictief moet worden uitgelegd.** Een dergelijke **bepaling kan dan ook niet rechtvaardigen dat** de in artikel 5 van richtlijn 2002/58 neergelegde **uitzondering** op de principiële verplichting om de vertrouwelijkheid van elektronische communicatie en daarmee verband houdende gegevens te waarborgen, en in het bijzonder op het verbod om deze gegevens op te slaan, **de regel wordt,** omdat laatstgenoemde bepaling anders grotendeels zou worden uitgehold (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 40 en aldaar aangehaalde rechtspraak).

58 Wat betreft de doelstellingen die een beperking van de onder meer in de artikelen 5, 6 en 9 van richtlijn 2002/58 neergelegde rechten en verplichtingen kunnen rechtvaardigen, heeft het Hof reeds geoordeeld dat de in artikel 15, lid 1, eerste volzin, van die richtlijn gegeven opsomming van **doelstellingen exhaustief is, zodat een op grond van deze bepaling vastgestelde wettelijke maatregel daadwerkelijk en strikt moet beantwoorden aan een van die doelstellingen** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 41 en aldaar aangehaalde rechtspraak).

59 Bovendien volgt uit artikel 15, lid 1, derde volzin, van richtlijn 2002/58 dat de **maatregelen** die de lidstaten krachtens deze bepaling treffen, **moeten stroken met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en de naleving van de door het Handvest gewaarborgde grondrechten moeten waarborgen.** In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronische-communicatiediensten opgelegde verplichting om verkeersgegevens te bewaren

teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot deze gegevens te verschaffen, **niet alleen vragen doet rijzen over de eerbiediging van de artikelen 7 en 8 van het Handvest, maar ook over de eerbiediging van artikel 11 van het Handvest,** dat betrekking heeft op de vrijheid van meningsuiting, die een van de wezenlijke grondslagen van een democratische en pluralistische samenleving is en behoort tot de waarden waarop de Europese Unie volgens artikel 2 VEU berust (zie in die zin arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punten 42 en 43 en aldaar aangehaalde rechtspraak).

60 In zoverre dient te worden **gepreciseerd dat de bewaring van verkeers- en locatiegegevens** als zodanig **niet alleen een uitzondering** op het in artikel 5, lid 1, van richtlijn 2002/58 neergelegde verbod op de opslag van deze gegevens door anderen dan de gebruikers vormt, **maar tevens een inmenging in de in de artikelen 7 en 8 van het Handvest erkende grondrechten op eerbiediging van het privéleven en bescherming van persoonsgegevens, ongeacht of de gegevens betreffende het privéleven gevoelig zijn, of de betrokkenen door die inmenging enig nadeel hebben ondervonden, en of de bewaarde gegevens vervolgens worden gebruikt** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 44 en aldaar aangehaalde rechtspraak).

61 Deze **gevolgtrekking is a fortiori gerechtvaardigd** omdat verkeers- en locatiegegevens informatie over een groot aantal aspecten van het privéleven van de betrokken personen aan het licht kunnen brengen, **waaronder gevoelige informatie zoals seksuele gerichtheid, politieke opvattingen, religieuze, filosofische, maatschappelijke of andersoortige overtuigingen en gezondheid**, terwijl dergelijke gegevens bovendien in het Unierecht bijzondere bescherming genieten. Op basis van deze gegevens, in hun geheel beschouwd, **kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren.** Met name kan aan de hand van deze gegevens het **profiel van de betrokken personen** worden opgesteld, informatie die vanuit het oogpunt van het recht op bescherming van het privéleven even gevoelig is als de inhoud zelf van de communicatie (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 45 en aldaar aangehaalde rechtspraak).

62 De **bewaring van verkeers- en locatiegegevens voor politiële doeleinden** kan dan ook **afbreuk doen aan het in artikel 7 van het Handvest neergelegde recht op eerbiediging van communicatie en kan de gebruikers van elektronische-communicatiemiddelen ervan weerhouden gebruik te maken van hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting, een ontradend effect dat des te sterker is naarmate de bewaarde gegevens talrijker en verscheidener zijn.** Daarbij komt dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard krachtens een algemene en ongedifferentieerde bewaringsmaatregel en op het gevoelige karakter van de informatie die uit deze gegevens kan worden afgeleid, **het enkele feit dat die gegevens worden bewaard door aanbieders van elektronische-communicatiediensten, risico's op misbruik en onrechtmatige**

toegang tot de gegevens in kwestie inhoudt (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 46 en aldaar aangehaalde rechtspraak).

63 Doordat artikel 15, lid 1, van richtlijn 2002/58 de lidstaten toestaat om de in de punten 51 tot en met 54 van het onderhavige arrest bedoelde rechten en verplichtingen te beperken, brengt deze bepaling tot uitdrukking dat de in de **artikelen 7, 8 en 11 van het Handvest erkende rechten niet absoluut zijn, maar moeten worden beschouwd in relatie tot hun functie in de samenleving**. Zoals blijkt uit artikel 52, lid 1, van het Handvest, staat het Handvest immers beperkingen op de uitoefening van die rechten toe, **mits deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van de rechten in kwestie eerbiedigen en – met inachtneming van het evenredigheidsbeginsel – 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.** Bij de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 in het licht van het Handvest moet bijgevolg **ook rekening worden gehouden met het belang dat toekomt aan de in de artikelen 3, 4, 6 en 7 van het Handvest neergelegde rechten en aan de doelstellingen van bescherming van de nationale veiligheid en bestrijding van zware criminaliteit als bijdrage tot de bescherming van de rechten en vrijheden van anderen** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 48 en aldaar aangehaalde rechtspraak).

64 Wat betreft met name de **effectieve bestrijding van strafbare feiten waarvan onder meer minderjarigen en andere kwetsbare personen het slachtoffer zijn,** moet dan ook in aanmerking worden genomen dat uit **artikel 7 van het Handvest positieve verplichtingen voor de overheid kunnen voortvloeien om juridische maatregelen te nemen ter bescherming van het privé- en het gezinsleven.** Tevens kunnen uit dat artikel **positieve verplichtingen** voortvloeien die betrekking hebben op de **bescherming van iemands woning en communicatie**, en kunnen uit de **artikelen 3 en 4 van het Handvest positieve verplichtingen voortvloeien die betrekking hebben op de bescherming van iemands lichamelijke en geestelijke integriteit alsook op het verbod op folteringen en onmenselijke of vernederende behandelingen** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 49 en aldaar aangehaalde rechtspraak).

65 Gelet op die verschillende positieve verplichtingen moeten de diverse **in het geding zijnde legitieme belangen en rechten dus met elkaar worden verzoend en moet een wettelijk kader tot stand worden gebracht dat dit mogelijk maakt** (zie in die zin arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C140/20, EU:C:2022:258, punt 50 en aldaar aangehaalde rechtspraak).

66 In dit verband vloeit uit de bewoordingen zelf van artikel 15, lid 1, eerste volzin, van richtlijn 2002/58 voort dat de lidstaten een maatregel die afwijkt van het in punt 52 van het onderhavige arrest vermelde vertrouwelijkheidsbeginsel, **kunnen treffen wanneer een dergelijke maatregel „in een democratische samenleving noodzakelijk, redelijk en proportioneel is", met dien verstande dat daarover in overweging 11 van die richtlijn staat te lezen dat zulke maatregel „strikt" evenredig moet zijn aan het nagestreefde doel.**

67 In zoverre zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de **uitzonderingen op en beperkingen van de bescherming van persoonsgegevens binnen de grenzen van het strikt noodzakelijke blijven.** Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder in aanmerking te nemen dat deze doelstelling moet worden verzoend met de grondrechten die bij de betreffende maatregel in het geding zijn, en dit via een evenwichtige afweging tussen de doelstelling van algemeen belang en de rechten in kwestie (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 52 en aldaar aangehaalde rechtspraak).

68 Meer bepaald volgt uit de rechtspraak van het Hof dat bij de beoordeling of de lidstaten een beperking van de onder meer in de artikelen 5, 6 en 9 van richtlijn 2002/58 neergelegde rechten en verplichtingen kunnen rechtvaardigen, moet worden vastgesteld hoe ernstig de uit deze beperking voortvloeiende inmenging is en moet worden nagegaan of het belang van de met die beperking nagestreefde doelstelling van algemeen belang in verhouding staat tot de ernst van die inmenging (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 53 en aldaar aangehaalde rechtspraak).

69 Een nationale wettelijke regeling voldoet slechts aan het **evenredigheidsvereiste indien zij duidelijke en nauwkeurige regels voor de reikwijdte en de toepassing van de maatregel in kwestie bevat waarbij minimumvereisten worden opgelegd,** zodat de personen van wie de persoonsgegevens in het geding zijn, beschikken over **voldoende waarborgen die een doeltreffende bescherming van deze gegevens tegen de risico's op misbruik mogelijk maken**. Die wettelijke regeling moet rechtens bindend zijn naar intern recht en met name vermelden in welke omstandigheden en onder welke voorwaarden een maatregel kan worden genomen die voorziet in de verwerking van die gegevens. **Aldus moet zij waarborgen dat de inmenging wordt beperkt tot het strikt noodzakelijke.** De **noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt**, met name wanneer er een aanzienlijk risico bestaat dat op onrechtmatige wijze toegang wordt verkregen tot die gegevens. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 54 en aldaar aangehaalde rechtspraak).

70 Een nationale wettelijke regeling die voorziet in de bewaring van persoonsgegevens, moet dan ook altijd beantwoorden aan **objectieve criteria waarbij een verband wordt gelegd tussen de te bewaren gegevens en het nagestreefde doel** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 55 en aldaar aangehaalde rechtspraak).

71 Wat betreft de **doelstellingen van algemeen belang** die een op grond van artikel 15, lid 1, van richtlijn 2002/58 genomen maatregel kunnen rechtvaardigen, blijkt uit de rechtspraak van het Hof en met name uit het arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791), dat er **overeenkomstig het evenredigheidsbeginsel een hiërarchie tussen die doelstellingen** bestaat op basis van hun respectieve belang en dat het belang van de met een dergelijke maatregel nagestreefde doelstelling in verhouding moet

staan tot de ernst van de uit de maatregel in kwestie voortvloeiende inmenging (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 56).

72 Wat betreft de **bescherming van de nationale veiligheid** – **die van groter belang is dan de overige in artikel 15, lid 1, van richtlijn 2002/58 genoemde doelstellingen** – heeft het Hof dan ook vastgesteld dat deze bepaling, gelezen in het licht van de artikelen 7, 8 en 11 alsook artikel 52, lid 1, van het Handvest, **zich niet verzet tegen wettelijke maatregelen** op grond waarvan aan aanbieders van elektronische-communicatiediensten, ten behoeve van de bescherming van de nationale veiligheid, **een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens kan worden gegeven in situaties waarin de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging voor de nationale veiligheid die reëel en actueel of voorzienbaar is, mits het besluit waarbij dit bevel wordt opgelegd, op doeltreffende wijze kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke entiteit waarvan de beslissing bindend is –** waarbij deze toetsing ertoe strekt na te gaan of een van die situaties zich voordoet en of de voorwaarden en waarborgen waarin moet worden voorzien in acht genomen zijn – **en mits dat bevel slechts kan worden uitgevaardigd voor een periode die niet langer is dan strikt noodzakelijk**, maar die kan worden verlengd als die bedreiging blijft bestaan (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 58 en aldaar aangehaalde rechtspraak).

73 Wat betreft de **doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen,** heeft het Hof erop gewezen dat **overeenkomstig het evenredigheidsbeginsel enkel de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen voor de openbare veiligheid een rechtvaardiging kunnen vormen voor ernstige inmengingen in de grondrechten die worden erkend in de artikelen 7 en 8 van het Handvest**, zoals de inmengingen waarmee de bewaring van verkeers- en locatiegegevens gepaard gaat. De **doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen kan bijgevolg slechts niet-ernstige inmengingen in die grondrechten rechtvaardigen** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 59 en aldaar aangehaalde rechtspraak).

74 Met betrekking tot de **doelstelling zware criminaliteit te bestrijden** heeft het Hof geoordeeld dat een nationale wettelijke regeling die daartoe een **algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens voorschrijft, verder gaat dan strikt noodzakelijk is en niet kan worden geacht gerechtvaardigd te zijn in een democratische samenleving**. Gezien het gevoelige karakter van de informatie die kan worden afgeleid uit verkeers- en locatiegegevens, is de vertrouwelijkheid van deze gegevens immers essentieel voor het recht op eerbiediging van het privéleven. Mede gelet op ten eerste het in punt 62 van het onderhavige arrest bedoelde ontradende effect dat de bewaring van die gegevens kan hebben op de uitoefening van de in de artikelen 7 en 11 van het Handvest neergelegde grondrechten, en ten tweede de ernst van de inmenging die deze bewaring met zich meebrengt, is het in een democratische samenleving dan ook van belang dat de **bewaring van verkeers- en locatiegegevens** – zoals in het bij richtlijn 2002/58 ingevoerde stelsel is bepaald – **de uitzondering en niet de regel vormt, alsmede dat die gegevens niet stelselmatig en continu**

kunnen worden bewaard. Deze **gevolgtrekking geldt zelfs ten aanzien van de doelstellingen die bestaan in de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen voor de openbare veiligheid,** alsmede ten aanzien van het belang dat aan deze doelstellingen moet worden toegekend (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 65 en aldaar aangehaalde rechtspraak).

75 Het Hof heeft evenwel verduidelijkt dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 alsook artikel 52, lid 1, van het Handvest, zich **niet verzet tegen wettelijke maatregelen die met het oog op de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen voor de openbare veiligheid voorzien in:**

– een gerichte bewaring van verkeers- en locatiegegevens die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk maar die kan worden verlengd;

– een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

– een algemene en ongedifferentieerde bewaring van de gegevens die betrekking hebben op de burgerlijke identiteit van de gebruikers van elektronische-communicatiemiddelen;

– de mogelijkheid om bij een aan effectieve rechterlijke toetsing onderworpen besluit van de bevoegde autoriteit aan aanbieders van elektronische-communicatiediensten een bevel te geven tot spoedbewaring (*quick freeze*), gedurende een bepaalde periode, van de verkeers- en locatiegegevens waarover zij beschikken,

mits die maatregelen, door middel van **duidelijke en nauwkeurige regels, waarborgen dat de gegevens in kwestie slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden is voldaan, en mits de betrokken personen beschikken over effectieve waarborgen tegen de risico's op misbruik** (arresten van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 168, en 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 67).

76 **In het licht van deze principiële overwegingen moeten de door de verwijzende rechter onder de aandacht gebrachte kenmerken van de in de hoofdgedingen aan de orde zijnde nationale regeling worden onderzocht.**

C. Systematisering standpunt HvJ

25. Uit deze arresten (onderstaande punten verwijzen naar het arrest HvJ SpaceNet) wordt voorafgaand op volgende principes, volgend uit artikel 15, lid 1 Richtlijn 2002/58/EG, gewezen voor wat betreft de beoordeling van de hier bestreden wet van 20 juli 2022:

(1) Essentieel is dat de maatregel noodzakelijk, redelijke en proportioneel is in een democratische samenleving en dat hij strikt evenredig is met het nagestreefde doel. Maatregel moet strikt noodzakelijk zijn. Maatregel moet proportioneel zijn wat duidelijke en nauwkeurige regels voor reikwijdte vereist (punt 66, 63, 67 en 69). Het betreft de vraag hoe ver de maatregel kan gaan om te oordelen of er (nog) sprake is van een democratische maatschappij, in tegenstelling tot dictaturen.

(2) Er moet rekening worden gehouden met de context, doelstellingen en totstandkomingsgeschiedenis van het Unierecht van E-privacy Richtlijn 2002/58/EG. (punt 49):
-vertrouwelijk karakter communicatie waarborgen (punt 51)
-in beginsel is opslaan gegevens zonder toestemming gebruiker verboden (punt 52)
-doelstelling: hoge mate van bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronische-communicatiediensten en eerbieding artikels 7 en 8 Handvest (punt 53)
-anonimiseren en wissen verkeersgegevens wanneer zij niet langer nodig zijn (punt 55)
-niet enkel toegang maar ook opslag waarborgen tegen misbruik (punt 56)
-maatregel mag beperking aan reikwijdte rechten opleggen maar moet uitzondering blijven en mag niet algemene regel zijn (punt 57)
-doelstellingen artikel 15.1 zijn exhaustief en maatregel moet daadwerkelijk en strikt beantwoorden aan die doelstellingen (punt 58)
-maatregel moet stroken met algemene beginselen Unierecht waaronder evenredigheidsbeginsel en waarborg rechten Handvest (punt 59)
-maatregel bewaren verkeers- en locatiegegevens is niet alleen uitzondering op artikel 5, lid 1 Richtlijn, maar is tevens een inmenging in artikel 7 en 8 Handvest (punt 60)
-verkeers- en locatiegegevens kunnen groot aantal aspecten uit privéleven – waaronder gevoelige informatie over seksuele gerichtheid, politieke opvattingen, religieuze, filosofische, maatschappelijke… overtuigingen – aan het licht brengen, en profiel betrokken personen opstellen (punt 61)
-bewaring verkeers- en locatiegegevens kan gebruikers ervan weerhouden gebruik te maken van vrijheid van meningsuiting, een ontradend effect dat des te sterker is naarmate bewaarde gegevens talrijker en verscheidener zijn (punt 62)

(3) Er is, overeenkomstig het evenredigheidsbeginsel, een hiërarchie tussen de doelstellingen van algemeen belang van artikel 15.1. (punt 71):

-doelstelling nationale veiligheid is van groter belang dan overige doelstellingen; ernstige bedreiging die reëel en actueel of voorzienbaar is kan aanleiding geven tot algemene en ongedifferentieerde bewaring, mits toetsing rechterlijke instantie of onafhankelijke bestuurlijke instantie en voor periode niet langer dan strikt noodzakelijk (punt 72)

-doelstelling strafbare feiten voorkomen, onderzoeken, opsporen, vervolgen overeenkomstig evenredigheidsbeginsel enkel de bestrijding van zware criminaliteit en voorkoming ernstige

bedreigingen voor de openbare veiligheid. Ernstige inmenging kan niet voor strafbare feiten in het algemeen (punt 73).

-doelstelling zware criminaliteit rechtvaardigt niet een algemene en ongedifferentieerde bewaring. Bewaring kan de uitzondering zijn, maar mag niet algemene regel worden en mag niet continu en stelselmatig gebeuren. (punt 74)

-dataretentie (g)een absolute noodzaak is voor de strafvervolging. De doeltreffendheid van strafvervolging hangt doorgaans niet af van één onderzoeksmiddel, maar van alle onderzoeksmiddelen waarover de bevoegde nationale autoriteiten te dien einde beschikken. (punt 96).

D. <u>Discussie en toepassing</u>

26. De bestreden wet van 20 april 2022 voert met de artikels 5, 6, 8, 9, 10, 11, 12 en 13 een geheel van maatregelen in die *de iure* en *de facto* een algemene bewaarplicht van communicatiegegevens invoert en een zeer brede toegang tot de bewaarde gegevens instelt. Vermelde artikels voeren in de wet van 13 juni 2005 betreffende de elektronische communicatie respectievelijk de artikels 122, 123, 126, 126/1, 126/2, 126/3 en 127 en 127/1 in.

    De artikels 5, 6, 8, 9, 10 en 12 van de wet van 20 april 2022 maken het mogelijk dat of verplichten aan de operatoren een groot aantal verkeers-, locatie- en identificatiegegevens te bewaren. Het merendeel van de verkeers- en locatiegegevens zijn als te bewaren opgenomen in deze wetsbepalingen; het gaat om ruim vijftig diverse gegevens. Zie tweede middel.

27. Artikel 11 van de wet van 20 april 2022 bepaalt vijf geografische zones waarin de gegevens onder bepaalde voorwaarden door de operatoren moeten bewaard worden. De bepalingen in de wet met betrekking tot deze geografische zones komen er op neer dat *de facto* het ganse grondgebied onder de verplichte bewaring kan vallen, en dit gedurende lange of onbepaalde periodes. Zie derde middel.

    Artikel 13 van de wet van 20 april 2022 bepaalt tien autoriteiten die onder bepaalde voorwaarden toegang kunnen krijgen tot de door de operatoren bewaarde gegevens. Het gaat om een zeer groot aantal autoriteiten en de meesten vallen buiten het kader van de doelstellingen van artikel 15.1 Richtlijn 2002/58/EG. Zo is zelfs een autoriteit betrokken die bevoegd is voor preventie, onderzoek, opsporing of vervolging van feiten die een strafrechtelijke inbreuk vormen, maar niet onder zware criminaliteit valt. Zie vierde middel.

28. De bestreden wet moet niet enkel in haar onderdelen (zie volgende middelen) maar ook in haar geheel beoordeeld worden. Het totaalplaatje van de wet maakt dat zowel op vlak van bewaring van gegevens als op vlak van toegang tot gegevens, en alleszins en minstens in de samenlezing van de bepalingen die er betrekking op hebben, de strijdigheid ervan met de vermelde principes zoals geformuleerd in het arrest HvJ SpaceNet onmiskenbaar is.

De algemeenheid van de maatregelen zowel wat betreft de bepalingen van te bewaren gegevens als wat betreft de bepalingen van toegang miskennen het evenredigheidsbeginsel en de verplichting van strikte evenredigheid met het nagestreefde doel. De maatregelen komen er op neer dat de uitzondering de regel wordt. Er wordt een veralgemeende en ongedifferentieerde bewaring ingevoerd. Zowat alle verkeers- en locatiegegevens worden bewaard; zowat het ganse grondgebied valt onder de bewaringsplicht; de locaties en infrastructuren opgenomen in de zones (artikel 126/2 §§3-5) omvatten quasi het ganse grondgebied. Een ruime groep van tien autoriteiten kan onder bepaalde voorwaarden toegang krijgen tot de gegevens. Dit gaat wat betreft de meerderheid van die autoriteiten voorbij aan de doelstellingen waarvoor op basis van artikel 15.1 Richtlijn 2002/58/EG bewaring en toegang mogelijk zijn. De hier bestreden wet ontwikkelt een systeem van continue en stelselmatige bewaring als algemene regel in het kader van de bewaring van gegevens inzake zware criminaliteit.

29. Zelfs in de uitzonderlijke situaties waarbij de rechtspraak van het HvJ algemene en ongedifferentieerde bewaring toelaat zijn de voorwaarden waaraan deze bewaring moet voldoen niet vervuld.

De bewaring in het kader van de nationale veiligheid op basis van het dreigingsniveau bepaald door OCAD voorziet niet in een toetsing door een rechterlijke instantie of een onafhankelijke bestuurlijke instantie, en bepaalt geen termijn van strikte noodzakelijkheid. Het dreigingsniveau beantwoordt niet aan de voorwaarde 'werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid'.

De bepalingen in verband met bewaring van gegevens in het kader van de zware criminaliteit gaat het kader van de zware criminaliteit ruim te buiten. Dit is nog flagranter waar de toegang tot de bewaarde gegevens in het kader van strafbare feiten zelfs niet formeel beperkt is tot zware criminaliteit, maar uitdrukkelijk ook feiten betreft die niet onder zware criminaliteit vallen. Bovendien wordt het begrip zware criminaliteit voor wat betreft de toegang tot de gegevens door de autoriteiten bevoegd voor preventie, onderzoek, opsporing en vervolging, veel ruimer bepaald dan de definitie van zware criminaliteit voor de bewaring van de gegevens. Terwijl voor bewaring (het al betwiste) artikel 90ter §§ 2 tot 4 wetboek strafvordering van toepassing wordt gesteld, geldt voor de toegang artikel 88bis §1 wetboek strafvordering (plus ook inbreuken Wetboek Economisch Recht en inzake Europese verordening machtsmisbruik) dat een veel lagere strafdrempel heeft dan artikel 90ter §§ 2 tot 4 wetboek strafvordering.

VI.2. TWEEDE MIDDEL

Geschonden wetsartikels en referentienormen

Schending van artikel 11, 12, 22 en 29 Grondwet.

Schending van artikel 15, lid 1 en de artikels 5, 6 en 9 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), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

Schending van artikel 6, 8, 10, 11 en 18 van het Europees Verdrag voor de bescherming van de Rechten van de Mens (EVRM).

Schending van de artikels 13 en 54 van de Richtlijn 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Geschonden referentienormen.

Recht op eerbiediging van de persoonlijke levenssfeer en bescherming van persoonlijke data, al dan niet in samenhang gelezen met het recht op vertrouwelijkheid van communicatie en met de algemene beginselen van informatieve zelfbeschikking en de beginselen van noodzaak in een democratische samenleving, legaliteit, proportionaliteit en subsidiariteit.

De schending van de in het middel vermelde wettelijke bepalingen door de artikels 122, 123, 126, 126/1 en 126/2, ingevoegd of gewijzigd door de artikels 5, 6, 8, 9 en 10 van de wet van 20 april 2022 in de wet van 13 juni 2005 betreffende elektronische communicatie, inhoudend de bepalingen van de gegevens die de operatoren verplicht moeten bewaard worden op zich of wanneer zij hiertoe verzocht worden. De te bewaren gegevens beantwoorden wat hun aantal en categorieën betreft niet aan de voorwaarden van proportionaliteit en noodzakelijkheid

A. Aangevochten wettelijke bepalingen

30. **Art. 122.§ 1. De operatoren verwijderen de verkeersgegevens met betrekking tot abonnees of eindgebruikers uit hun verkeersgegevens of maken deze gegevens anoniem, zodra zij niet langer nodig zijn voor de transmissie van de communicatie.**
§ 2. In afwijking van paragraaf 1 en met als enig doel de facturering van abonnees of het doen van interconnectie betalingen, mogen de operatoren de daartoe noodzakelijke verkeersgegevens bewaren en verwerken.

Onverminderd de toepassing van de AVG en van de wet van 30 juli 2018 stelt de operator de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben, voorafgaand aan de verwerking in kennis van :

1° de soorten verkeersgegevens die worden verwerkt;

2° de precieze doeleinden van de verwerking;

3° de duur van de verwerking.

De verwerking van de gegevens bedoeld in het eerste lid, is slechts toegestaan tot het einde van de periode van de betwisting van de factuur of tot het einde van de periode waarin de betaling gerechtelijk kan worden afgedwongen.

§ 3. In afwijking van § 1 en met als enig doel de marketing te verzorgen van de eigen elektronische-communicatiediensten het gebruikspatroon bedoeld in artikel 110, § 4, eerste lid, artikel 110/1 en artikel 111, § 3, tweede lid, op te stellen, of diensten met verkeersgegevens of locatiegegevens te leveren, mogen de operatoren de in § 1 bedoelde gegevens slechts verwerken onder de volgende voorwaarden :

1° De operator stelt de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben, voorafgaand aan het verkrijgen van diens toestemming voor de verwerking, in kennis van :

a) de soorten verkeersgegevens die worden verwerkt;

b) de precieze doeleinden van de verwerking;

c) de duur van verwerking.

2° De abonnee of, in voorkomend geval, de eindgebruiker, heeft voorafgaand aan de verwerking zijn toestemming gegeven voor de verwerking.

Onder toestemming voor de verwerking in de zin van dit artikel wordt verstaan de toestemming in de zin van artikel 4, 11), van de AVG.

3° De betrokken operator biedt zijn abonnees of eindgebruikers gratis de mogelijkheid om makkelijk en te allen tijde de gegeven toestemming in te trekken.

4° De verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de levering van de betrokken dienst met verkeersgegevens of locatiegegevens voor het opstellen van het gebruikspatroon bedoeld in artikel 110, § 4, eerste lid, artikel 110/1 en artikel 111, § 3, tweede lid, of voor de marketingactie in kwestie.

Deze voorwaarden zijn van toepassing onverminderd de bijkomende voorwaarden die voortvloeien uit de toepassing van de AVG en van de wet van 30 juli 2018.

§ 4. In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen en om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, en voor zover hij deze verwerkt of genereert in het kader van de verstrekking van dat netwerk of van die dienst:

1° bewaart de operator, in het kader van de verstrekking van een interpersoonlijke communicatiedienst en gedurende vier maanden vanaf de datum van de communicatie, de daartoe noodzakelijke verkeersgegevens onder de volgende verkeersgegevens:

- de identifier van de bron van de communicatie;

- de identifier van de bestemming van de communicatie;

- de precieze datums en tijdstippen van het begin en het einde van de communicatie;

- de locatie van de eindapparatuur van de communicerende partijen bij de aanvang en bij het einde van de communicatie;

2° bewaart de operator gedurende twaalf maanden vanaf de datum van de communicatie de

volgende verkeersgegevens betreffende de binnenkomende communicatie in het kader van de verstrekking van interpersoonlijke communicatiediensten, teneinde de persoon die de communicatie doet, te identificeren:

- het telefoonnummer aan de bron van de binnenkomende communicatie, of;

- het IP-adres dat werd gebruikt om de binnenkomende communicatie te versturen, het tijdstempel en de gebruikte poort, en;

- de precieze datums en tijdstippen van begin en einde van de binnenkomende communicatie;

3° bewaart de operator de in 1° bedoelde gegevens die betrekking hebben op een specifieke geïdentificeerde fraude of een specifiek geïdentificeerd kwaadwillig gebruik van het netwerk gedurende de periode die nodig is voor de analyse en het verhelpen ervan, in voorkomend geval langer dan de termijn van vier maanden bedoeld in 1° ;

4° bewaart de operator de verkeersgegevens bedoeld in 2° en met betrekking tot een specifiek kwaadwillig gebruik van het netwerk gedurende de periode die nodig is voor de verwerking van dit kwaadwillig gebruik, in voorkomend geval langer dan de termijn van twaalf maanden bedoeld in 2° ;

5° verwerkt de operator de noodzakelijke verkeersgegevens voor deze doeleinden, met inbegrip van de gegevens bedoeld in paragraaf 2 indien nodig.

In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen, om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, mag de operator andere gegevens dan deze bedoeld in het eerste lid bewaren en verwerken, die voor deze doeleinden nodig worden geacht.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Gegevensbeschermingsautoriteit, de verkeersgegevens waarvan de bewaring als noodzakelijk moet worden beschouwd voor het nastreven van de in deze paragraaf bedoelde doeleinden, preciseren en uitbreiden.

In geval van vermeende fraude of van vermeend kwaadwillig gebruik, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de vermeende fraude of het vermeende kwaadwillig gebruik doorsturen.

§ 4/1. In afwijking van paragraaf 1 mogen de operatoren die verkeersgegevens bewaren en verwerken die nodig zijn om de veiligheid en correcte werking van hun elektronische-communicatienetwerken en -diensten te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren.

De operatoren mogen deze bewaren voor een duur van twaalf maanden vanaf de datum van de communicatie.

De operatoren mogen de in het eerste lid bedoelde gegevens met betrekking tot een specifieke schending van de veiligheid van het netwerk bewaren gedurende de periode die nodig is om deze te behandelen, in voorkomend geval langer dan de termijn van twaalf maanden bedoeld in het tweede lid.

In geval van schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten doorsturen.

§ 4/2. In afwijking van paragraaf 1 bewaren en verwerken de operatoren de verkeersgegevens die

nodig zijn om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm, voor de daartoe benodigde duur.

§ 5.De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de facturering of het beheer van het verkeer, de behandeling van verzoeken om inlichtingen van abonnees, de bestrijding van fraude of het kwaadwillig gebruik van het netwerk, de veiligheid van het netwerk, de naleving van zijn wettelijke verplichtingen, de marketing van de eigen elektronische-communicatiediensten of de levering van diensten die gebruik maken van verkeersgegevens of locatiegegevens en door de leden van zijn Coördinatiecel bedoeld in artikel 127/3.

§ 6. Het Instituut, de Ombudsdienst voor telecommunicatie, de Belgische Mededingingsautoriteit], de rechtscolleges van de rechterlijke orde en de Raad van State kunnen in het kader van hun bevoegdheden in kennis worden gesteld van de relevante verkeers- en rekeninggegevens met het oog op het beslechten van geschillen, waaronder geschillen met betrekking tot interconnectie en facturering.

Art. 123.§ 1. Onverminderd de toepassing van de AVG en van de wet van 30 juli 2018 mogen de operatoren van mobiele netwerken andere locatiegegevens dan verkeersgegevens die betrekking hebben op een abonnee of een eindgebruiker slechts bewaren en verwerken in de volgende gevallen:

1° wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst, waarbij de gegevens worden bewaard gedurende maximaal twaalf maanden vanaf de datum van de communicatie, tenzij in geval van een specifieke schending van de veiligheid van het netwerk waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;

2° wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren, waarbij de gegevens worden bewaard gedurende maximaal vier maanden vanaf de datum van de communicatie, tenzij in geval van specifieke fraude of specifiek kwaadwillig gebruik waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;

3° wanneer de gegevens anoniem gemaakt zijn;

4° wanneer de verwerking past in het kader van de levering van een dienst die gebruik maakt van verkeersgegevens of locatiegegevens;

5° wanneer de verwerking noodzakelijk is om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm.

§ 2. De verwerking in het kader van de levering van een dienst gebaseerd op verkeersgegevens of locatiegegevens is onderworpen aan de volgende voorwaarden :

1° De operator stelt de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben, voorafgaand aan het verkrijgen van diens toestemming voor de verwerking in kennis van :

a) de soorten locatiegegevens die worden verwerkt;

b) de precieze doeleinden van de verwerking;

c) de duur van de verwerking;

d) de eventuele derden waaraan deze gegevens zullen worden doorgegeven;

e) de mogelijkheid om te allen tijde de gegeven toestemming voor de verwerking definitief of tijdelijk in te trekken.

2° De abonnee of, in voorkomend geval, de eindgebruiker, heeft voorafgaand aan de verwerking

zijn toestemming gegeven voor de verwerking.

Onder toestemming voor de verwerking in de zin van dit artikel wordt verstaan de toestemming in de zin van artikel 4, 11), van de AVG.

3° De verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de levering van de betrokken dienst met verkeersgegevens of locatiegegevens.

4° De betrokken operator biedt zijn abonnees of eindgebruikers gratis de mogelijkheid om te allen tijde op eenvoudige wijze de gegeven toestemming, definitief of tijdelijk, in te trekken.

§ 4. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die werkzaam zijn in opdracht van de operator of de derde die de dienst die gebruik maakt van verkeersgegevens of locatiegegevens levert, of door de Coördinatiecel van de operator bedoeld in artikel 127/3.

De verwerking is beperkt tot hetgeen strikt noodzakelijk is om de betrokken dienst met verkeersgegevens of locatiegegevens aan te kunnen bieden.

§ 5. In geval van een noodcommunicatie naar de beheercentrales van de nooddiensten die ter plaatse hulp bieden, heffen de operatoren in zoverre dit technisch mogelijk is, met als doel de behandeling van de noodcommunicatie door de betrokken beheercentrales mogelijk te maken, de tijdelijke weigering of het ontbreken van toestemming van de abonnee of de eindgebruiker betreffende de verwerking van lokalisatiegegevens per afzonderlijke, oproepende lijn, op.

Die opheffing is gratis

Art. 126. § 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische-communicatienetwerken aanbieden waarmee deze diensten verstrekt kunnen worden, de volgende gegevens, voor zover ze die verwerken of genereren in het kader van de verstrekking van die netwerken of diensten:

1° het Rijksregisternummer of een equivalent nummer, de naam en voornaam van de eindgebruiker die een natuurlijke persoon is of de naam van de abonnee die een rechtspersoon is;

2° de eventuele alias gekozen door de eindgebruiker bij de inschrijving op of de activering van de dienst;

3° de contactgegevens van de abonnee die verstrekt zijn bij de inschrijving op de dienst, met name zijn telefoonnummer, zijn e-mailadres en zijn postadres;

4° de datum en het tijdstip van inschrijving op de dienst en van de activering van de dienst en de elementen aan de hand waarvan de plaats kan bepaald worden waarvandaan die inschrijving en die activering zijn uitgevoerd, met name:

- het fysieke adres van het verkooppunt waar de inschrijving of activering heeft plaatsgevonden, of;

- het fysieke adres van het netwerkaansluitpunt dat gediend heeft voor de inschrijving of de activering, of;

- het IP-adres dat gediend heeft voor de inschrijving of de activering, alsook de bronpoort van de verbinding en het tijdstempel, of;

- in het kader van een mobiel telefoonnetwerk, de geografische locatie van de eindapparatuur die de inschrijving of de activering aan de hand van een telefoonnummer mogelijk heeft gemaakt;

5° het fysieke leveringsadres van de dienst;

6° het facturatieadres van de dienst en de gegevens betreffende de betalingswijze en het betaalmiddel, het tijdstip van de betalingen en de referentie van de betalingstransactie in geval

van onlinebetaling;

7° de hoofddienst en de aanvullende diensten die de abonnee kan gebruiken;

8° de datum vanaf wanneer die diensten gebruikt kunnen worden, de datum van het eerste gebruik van die diensten en de datum van beëindiging van die diensten;

9° in geval van overdracht van de identifier van de abonnee, zoals zijn telefoonnummer, de identiteit van de operator die de identifier overdraagt en de identiteit van de operator naar wie de identifier wordt overgedragen en de datum waarop de overdracht wordt uitgevoerd;

10° het toegewezen telefoonnummer;

11° het voornaamste e-mailadres en de e-mailadressen die als alias gebruikt worden;

12° de internationale identiteit van de mobiele abonnee, "International Mobile Subscriber Identity", afgekort "IMSI";

13° de permanente identifier van het abonnement, "Subscription Permanent Identifier", afgekort "SUPI";

14° de verdoken identifier van het abonnement, "Subscription Concealed Identifier", afgekort "SUCI";

15° het IP-adres aan de bron van de verbinding, het tijdstempel van de toewijzing alsook, in geval van gedeeld gebruik van een IP-adres van de eindgebruiker, de poorten die daaraan zijn toegewezen;

16° de identifier van de eindapparatuur van de eindgebruiker, of indien de operator dit niet verwerkt of genereert, de identifier van de apparatuur die zich het dichtste bij die eindapparatuur bevindt, met name:

- de internationale identiteit van de mobiele apparatuur, "International Mobile Equipment Identity", afgekort "IMEI";

- de permanente identifier van de apparatuur, "Permanent Equipment Identifier", afgekort "PEI";

- het adres van de controller van de toegang tot het netwerk, "Media Access Control address", afgekort "MAC";

17° de andere identifiers met betrekking tot de eindgebruiker, tot de eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning bepaald worden, op voorwaarde dat dit besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

De operatoren hoeven de MAC-adressen bedoeld in het eerste lid, 16°, derde streepje, niet te bewaren voor de elektronische-communicatiediensten die ze enkel aan ondernemingen of rechtspersonen aanbieden.

Het koninklijk besluit bedoeld in het eerste lid, 17°, slaat niet op de inhoud van de elektronische communicatie, noch op de elektronische-communicatie metagegevens die informatie geven over de geadresseerde van de communicatie, zoals het IP-adres van de geadresseerde van de communicatie, of over de locatie van de eindapparatuur.

De Koning:

1° kan de gegevens bedoeld in het eerste lid preciseren;

2° bepaalt de vereisten inzake nauwkeurigheid en betrouwbaarheid waaraan deze gegevens moeten beantwoorden.

§ 2. De operatoren bewaren de in paragraaf 1, eerste lid, 1° tot 14°, bedoelde gegevens tot zolang de elektronische-communicatiedienst gebruikt wordt en tot twaalf maanden na het einde van de dienst.

De operatoren bewaren de in paragraaf 1, eerste lid, 15° en 16°, bedoelde gegevens gedurende

een periode van twaalf maanden na het einde van de sessie.

In afwijking van het tweede lid wordt de bewaringstermijn van de in paragraaf 1, eerste lid, 16°, derde streepje, bedoelde gegevens, teruggebracht tot zes maanden na het einde van de sessie indien de operator een ander gegeven zoals bedoeld in paragraaf 1, eerste lid, 16°, bewaart.

De operatoren bewaren de gegevens bedoeld in paragraaf 1, eerste lid, 17°, gedurende de door de Koning bepaalde periode. Die periode mag niet langer zijn dan de in het eerste lid bedoelde bewaringstermijn.

Het koninklijk besluit bedoeld in paragraaf 1, eerste lid, 17°, en vierde lid, en in paragraaf 2, vierde lid, wordt voorgesteld door de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, maakt het voorwerp uit van een advies van de Gegevensbeschermingsautoriteit en van het Instituut en daarover wordt beraadslaagd in de Ministerraad.

Art. 126/1. § 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische- communicatiediensten aanbieden, alsook de operatoren die onderliggende en elektronische-communicatienetwerken aanbieden, de in artikel 126/2, § 2, bedoelde gegevens voor de geografische zones bedoeld in artikel 126/3, gedurende twaalf maanden te rekenen vanaf de datum van de communicatie, tenzij een andere termijn bepaald is in artikel 126/3.

Elke operator bewaart de gegevens die door hem gegenereerd of verwerkt zijn in het kader van de verstrekking van de betrokken van de verstrekking van de betrokken elektronische-communicatiediensten en -netwerken.

Deze gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon.

§ 2. De elektronische-communicatie metagegevens, met inbegrip van de metagegevens voor de oproeppogingen zonder resultaat, waarop de in paragraaf 1 bedoelde bewaarplicht van toepassing is, worden opgesomd in artikel 126/2, § 2.

§ 3. De operatoren bewaren de verkeersgegevens voor iedere communicatie of alle oproeppogingen zonder resultaat die vanuit of naar een geografisch gebied als bedoeld in artikel 126/3 worden gevoerd.

Indien de operator, als gevolg van de door hem gebruikte technologie, niet in staat is de eindapparatuur die betrokken is bij de communicatie, met inbegrip van de oproeppoging zonder resultaat, nauwkeuriger te lokaliseren dan de lokalisatie ervan op het nationale grondgebied, bewaart de operator de in artikel 126/2, § 2, bedoelde gegevens gedurende de kortste overeenkomstig dit artikel en artikel 126/3 bepaalde termijn, op voorwaarde dat overeenkomstig dit artikel en artikel 126/3 het gehele nationale grondgebied gedekt is door een bewaarplicht. Indien niet aan deze voorwaarde is voldaan, bewaart de operator op wie dit lid van toepassing is deze gegevens niet.

Wanneer de eindgebruiker zich tijdens een elektronische communicatie verplaatst, bewaart de operator de verkeersgegevens voor zover de eindgebruiker zich op een bepaald moment van de communicatie bevindt in een zone bedoeld in artikel 126/3.

De operatoren bewaren de gegevens met betrekking tot de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het

netwerkaansluitpunt, die opgesomd zijn in artikel 126/2, § 2, wanneer die apparatuur zich bevindt in een in artikel 126/3 bedoelde zone.

Om te bepalen of eindapparatuur zich in een geografische zone als bedoeld in artikel 126/3 bevindt, maken de operatoren gebruik van de meest betrouwbare en nauwkeurige gegevens als mogelijk is. Zij maken hiervoor, indien beschikbaar, gebruik van de satellietlocatie van eindapparatuur.

Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot een in artikel 126/3 bedoelde zone, bewaart hij de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden.

Wanneer een aggregatiepunt van de operator, zoals een antenne, verschillende in artikel 126/3 bedoelde geografische zones dekt die onderworpen zijn aan een verschillende bewaringstermijn, bewaart de operator de gegevens voor dat aggregatiepunt gedurende de kortste bewaringstermijn.

Wanneer op grond van dit artikel en van artikel 126/3 verschillende bewaringstermijnen van toepassing zijn op dezelfde gegevens, bewaren de operatoren de gegevens gedurende de kortste termijn.

§ 4. De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie, en van de minister, na raadpleging van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, het volgende bepalen:

- de technische parameters en gegevens die de operatoren gebruiken om de gegevensopslag te beperken tot de in artikel 126/3 bedoelde zones;

- de lijst van de verschillende autoriteiten die bevoegd zijn voor de in artikel 126/3, §§ 2 tot 5, bedoelde aangelegenheden;

- de nadere regels voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst, de nadere regels voor de mededeling van informatie door deze dienst aan de betrokken operatoren en de termijn waarbinnen de operatoren jaarlijks de in paragraaf 1 bedoelde bewaring ten uitvoer leggen;

- in voorkomend geval, de bijkomende geografische zones bedoeld in artikel 126/3, § 3, m), § 4, g), en § 5, f).

Het koninklijk besluit bedoeld in het eerste lid, vierde streepje, wordt elke drie jaar hernieuwd. Bij ontstentenis van een hernieuwing vervalt de verplichting tot bewaring bedoeld in paragraaf 1 wat deze bijkomende geografische zones betreft, en dit tot een nieuw koninklijk besluit van kracht wordt.

§ 5. De minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister brengen, na voorafgaand advies van het Coördinatiecomité Inlichtingen en Veiligheid, van het Instituut en de autoriteiten bevoegd voor de bescherming van de gegevens, jaarlijks een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel en, in voorkomend geval, van het in paragraaf 4 bedoelde koninklijk besluit, teneinde na te gaan of het nodig is bepalingen aan te passen.

In dit evaluatieverslag wordt in het bijzonder nagegaan of de categorieën van geografische zones opgenomen in de wet en het in paragraaf 4 bedoelde koninklijk besluit nog steeds voldoen aan de criteria bedoeld in artikel 126/3, §§ 3 tot 5, en of het nog nodig is deze te handhaven dan wel of andere categorieën opgenomen moeten worden.

Categorieën van geografische zones kunnen enkel opgenomen worden ter vrijwaring van de nationale veiligheid, of indien er in deze zones op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico op het voorbereiden of plegen van daden van zware criminaliteit.

Het evaluatieverslag bevat ook het percentage van het nationale grondgebied waarvoor de verplichting tot gegevensbewaring op basis van dit artikel en artikel 126/3 van toepassing is.

Dit evaluatieverslag wordt gestuurd naar het Controleorgaan op de politionele informatie en naar het Vast Comité I.

Art. 126/2. § 1. Voor de toepassing van dit artikel wordt verstaan onder "communicatie", informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een publiek beschikbare elektronische-communicatiedienst, met uitsluiting van de informatie die via een openbare omroepdienst over een elektronische-communicatienetwerk wordt overgebracht, behalve in de mate waarin de informatie kan worden gelinkt aan de identificeerbare abonnee of gebruiker die deze informatie ontvangt.

§ 2. De gegevens bedoeld in artikel 126/1, § 2, die in uitvoering van de artikelen 126/1 en 126/3 bewaard moeten worden door de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook door de operatoren die de onderliggende elektronische-communicatienetwerken aanbieden die het aanbieden van die diensten mogelijk maken, zijn de volgende:

1° de beschrijving en de technische karakteristieken van de elektronische-communicatiedienst die werd aangewend tijdens de communicatie;

2° de identificatiegegevens bedoeld in artikel 126, § 1, 2°, 10° tot 14°, en 16°, van de geadresseerde van de communicatie;

3° voor de elektronische-communicatiediensten met uitzondering van de internettoegangsdiensten, het IP-adres dat gebruikt is door de geadresseerde van de communicatie, het tijdstempel alsook, in geval van gedeeld gebruik van een IP-adres van de geadresseerde, de poorten die aan hem zijn toegewezen;

4° in geval van een groepsgesprek, oproepdoorschakeling of -doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;

5° de datum en het exacte tijdstip van de aanvang en het einde van de sessie van de betrokken elektronische-communicatiedienst, waaronder de datum en het exacte tijdstip van de aanvang en het einde van de oproep;

6° de gegevens die de identificatie en de lokalisatie van de cellen of andere netwerkaansluitpunten van het mobiele netwerk mogelijk maken, die werden gebruikt voor de communicatie, van de start tot het einde van de communicatie, alsook de exacte data en tijdstippen van deze verschillende locaties;

7° het tijdens de duur van de sessie geüploade en gedownloade volume van gegevens;

8° voor wat betreft de mobiele elektronische-communicatiediensten, de datum en het tijdstip van de verbinding van de eindapparatuur met het netwerk wegens het opstarten van die apparatuur, en het moment waarop de verbinding van deze eindapparatuur met het netwerk wordt verbroken wegens het uitschakelen van die apparatuur;

9° voor wat betreft de mobiele elektronische-communicatiediensten, de locatie van de eindapparatuur en de datum en het tijdstip van deze locatie telkens wanneer de operator wil

weten welke eindapparatuur is verbonden met zijn netwerk;

10° de andere identifiers met betrekking tot de geadresseerde van de elektronische communicatie, tot zijn eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning bepaald worden, na advies van de Gegevensbeschermingsautoriteit en het Instituut, op voorwaarde dat dit besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

In afwijking van de artikelen 126/1 en 126/3 bedraagt de bewaartermijn van het gegeven bedoeld in het eerste lid, 8°, zes maanden nadat het is gegenereerd of verwerkt.

Het koninklijk besluit bedoeld in het eerste lid, 10°, slaat niet op de inhoud van de elektronische communicatie.

De Koning kan, na advies van de Gegevens-beschermingsautoriteit en het Instituut, de gegevens bedoeld in eerste lid, preciseren.

§ 3. De combinatie van de gegevens bewaard in uitvoering van artikel 126 en van dit artikel moet het mogelijk maken om de relatie te leggen tussen de bron en de bestemming van de communicatie.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, en na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, de vereisten inzake nauwkeurigheid en betrouwbaarheid bepalen waaraan de gegevens bedoeld in dit artikel moeten beantwoorden.

<u>Art. 127.</u> § 1. Dit artikel is van toepassing op de operatoren die in België een elektronische-communicatiedienst aanbieden aan eindgebruikers. …

§ 6. De toegestane identificatiedocumenten ter identificatie van de abonnee die een natuurlijke persoon is, zijn de volgende:

1° de Belgische elektronische identiteitskaart;

2° het Belgisch paspoort;

3° het bewijs van inschrijving in het vreemdelingenregister - tijdelijk verblijf, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (A-kaart);

4° de beperkte verblijfstitel (A-kaart);

5° het bewijs van inschrijving in het vreemdelingenregister, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (B-kaart);

6° de onbeperkte verblijfstitel (B-kaart);

7° de identiteitskaart voor vreemdelingen, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (C-kaart);

8° de vestigingsvergunning (K-kaart);

9° de EU-verblijfstitel voor langdurig ingezetenen, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (D-kaart);

10° de EU-verblijfstitel voor langdurig ingezetenen (L-kaart);

11° de verklaring van inschrijving, afgeleverd voor 10 mei 2021, op voorwaarde dat deze nog steeds geldig is (E-kaart);

12° het document van inschrijving "Art. 8 RL 2004/38/EG" E (EU-kaart);

13° het document ter staving van duurzaam verblijf, afgeleverd voor 10 mei 2021, op voorwaarde dat deze nog steeds geldig is (E+-kaart);

14° het document van duurzaam verblijf "Art. 19 RL 2004/38/EG" (EU+-kaart);

15° de verblijfskaart van een familielid van een burger van de Unie, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (F-kaart);

16° de verblijfskaart van een familielid van een burger van de Unie "familielid EU - Art. 10 RL 2004/38/EG" (F-kaart);

17° de duurzame verblijfskaart van een familielid van een burger van de Unie, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (F+-kaart);

18° de duurzame verblijfskaart van een familielid van een burger van de Unie "Familielid EU - Art. 20 RL 2004/38/EG" (F+-kaart);

19° de Europese blauwe kaart (H-kaart);

20° de vergunning voor een binnen een onderneming overgeplaatste persoon "ICT" (I-kaart);

21° de vergunning voor lange-termijnmobiliteit "mobiele ICT" (J-kaart);

22° de verblijfskaart voor begunstigden van het terugtrekkingsakkoord "Artikel 50 VEU" (M-kaart);

23° de duurzame verblijfskaart voor begunstigden van het terugtrekkingsakkoord "Artikel 50 VEU" (M-kaart);

24° de kaart voor klein grensverkeer voor begunstigden van het terugtrekkingsakkoord "Artikel 50 VEU - grensarbeider" (N-kaart);

25° de akte van bekendheid;

26° de bijlage 12 verstrekt krachtens artikel 6 van het koninklijk besluit van 25 maart 2003 betreffende de identiteitskaarten of krachtens artikel 36bis van het koninklijk besluit van 8 oktober 1981 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen;

27° het attest van immatriculatie (oranje kaart);

28° de buitenlandse identiteitskaart, wanneer een internationaal paspoort niet nodig is om in België te verblijven;

29° de bijzondere identiteitskaarten verstrekt aan de categorieën van personeel dat actief is in diplomatieke en consulaire zendingen en aan hun familieleden, krachtens de Verdragen van Wenen van 1961 en 1963 en het koninklijk besluit van 30 oktober 1991 betreffende de documenten voor het verblijf in België van bepaalde vreemdelingen;

30° de identiteitskaart verstrekt conform de Conventies van Genève van 12 augustus 1949 inzake de bescherming van de slachtoffers van internationale gewapende conflicten;

31° het buitenlands paspoort;

32° elk ander document bepaald door de Koning, op voorwaarde dat het koninklijk besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit…

§7. Onverminderd artikel 126 bewaart de operator het rijksregisternummer, de naam en voornaam van zijn abonnee die een natuurlijke persoon is, wanneer hij die abonnee identificeert aan de hand van zijn Belgische elektronische identiteitskaart.

Onverminderd artikel 126 bewaart de operator, bij het identificeren van de abonnee via een ander document dan de Belgische elektronische identiteitskaart of aan de hand van een andere directe identificatiemethode dan de overlegging van een identificatiedocument, tussen de volgende gegevens diegene die op het voorgelegde identificatiedocument staan of diegene die worden verwerkt tijdens de toepassing van de directe identificatiemethode:

1° de naam en voornaam;

2° de nationaliteit;

3° de geboortedatum;

4° het adres van de woonplaats, het e-mailadres en het telefoonnummer;

5° het nummer van het identificatiedocument en het land van uitgifte van het document wanneer het een buitenlands document betreft;

6° het verband tussen de nieuwe elektronische-communicatiedienst waarop de abonnee intekent en de dienst waarvoor hij reeds werd geïdentificeerd.

§ 8. Wanneer een operator op basis van een voorafbetaalde kaart een mobiele elektronische-communicatiedienst aanbiedt aan een abonnee die een rechtspersoon is en die hij identificeert aan de hand van een directe identificatiemethode, vergaart en bewaart hij de burgerlijke identiteit van een natuurlijke persoon die handelt voor rekening van de rechtspersoon, conform de vereisten bedoeld in de paragrafen 4 tot 7.…

§ 10. De operator maakt het voor de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid, mogelijk om zijn abonnees te identificeren via een indirecte identificatiemethode:

1° door de bewaring, overeenkomstig artikel 126 en gedurende de in dat artikel bepaalde termijnen, van het IP-adres dat werd gebruikt om zich op de elektronische-communicatiedienst in te tekenen of om deze dienst te activeren, het IP-adres aan de bron van de verbinding en de gegevens die daarbij bewaard moeten worden, of;

2° door de vergaring en bewaring van het telefoonnummer van de abonnee dat werd toegewezen in het kader van een elektronische-communicatiebetaaldienst waarvoor een operator de abonnee moet identificeren krachtens dit artikel, of;

3° in geval van een onlinebetaling specifiek voor de intekening op een elektronische-communicatiedienst, door de vergaring en bewaring van:

- het kenmerk van de betalingsverrichting, en;

- de naam, de voornaam, het verblijfadres en de geboortedatum opgegeven door de natuurlijke persoon die de abonnee van de operator is of die handelt voor rekening van een rechtspersoon die de abonnee van de operator is, teneinde zijn verplichtingen inzake identificatie te vervullen, of;

4° in geval van een simkaart ("subscriber identity/identification module") of andere gelijkwaardige kaart die in een voertuig wordt ingebouwd, door de vergaring en bewaring van het chassisnummer van het voertuig en van de link tussen het chassisnummer en het nummer van de kaart;

5° in geval van een intekening van een abonnee die in een gesloten centrum of woonunit verblijft in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op een mobiele elektronische-communicatiedienst verstrekt door middel van een voorafbetaalde kaart, door de vergaring en bewaring van de naam en de voornaam van de abonnee, zijn openbaar veiligheidsnummer, zijnde het door de Dienst Vreemdelingenzaken toegekende dossiernummer, en de contactgegevens van het centrum of de woonunit waar de intekening heeft plaatsgevonden, of:

6° in geval van intekening op een elektronische-communicatiedienst door een rechtspersoon namens en voor rekening van een natuurlijke persoon die moeilijkheden heeft om die intekening te verrichten, door de vergaring en bewaring van de precieze benaming van de rechtspersoon en, wat de natuurlijke persoon in kwestie betreft, minimaal zijn naam, zijn voornaam, zijn verblijfadres

als hij dat heeft, zijn geboortedatum en het nummer op basis waarvan hij is geïdentificeerd, zoals een rijksregisternummer, welke hem wordt meegedeeld door de rechtspersoon. …

§ 11. Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.
… De operator die een simkaart of een gelijkwaardige kaart aanbiedt die bestemd is om in een voertuig te worden ingebouwd, bewaart het chassisnummer van dat voertuig, evenals de link tussen het chassisnummer en het nummer van deze kaart. Op verzoek van een autoriteit deelt de operator haar enkel dat chassisnummer of het nummer van deze kaart mee.

B. Systematisering van de te bewaren gegevens

31. Door de geciteerde artikels heeft de wetgever een complex systeem verordend voor wat betreft de door de operatoren te bewaren gegevens, zowel wat betreft de aard en omvang van de gegevens, als wat betreft de mogelijkheid tot bewaring enerzijds en de verplichting tot bewaring anderzijds, en eveneens wat betreft de verplichting de gegevens te bewaren voor eigen gebruik en/of met het oog op opvraging door bepaalde overheden.

32. De essentiële kwestie in het kader van dit onderdeel van het middel betreft de aard en omvang van de (al of niet verplicht) bewaarde gegevens. Dit staat op zich los van de (overigens verschillende) termijnen gedurende dewelke de gegevens moeten bewaard worden. Dit staat op zich los van het gegeven dat de data bewaard worden voor facturering, interconnectiebetalingen, marketing, vaststellen fraude of kwaadwillig gebruik van het netwerk of de verwerking van de bewaarde gegevens. Dit staat op zich los van de situaties waarbij op basis van plaatsen en zones (artikel 126/3) gegevens moeten bewaard worden. Dit staat op zich ook los van de overheden aan wie de data eventueel moeten overgemaakt worden (artikel 127/1).

33. In essentie komt de wettelijke regeling neer op het volgende.

-Geen bewaring van inhoud communicatie.

-Wel bewaring van verkeers-, locatie- en identiteitsgegevens, die idee kunnen geven over aard en inhoud van communicatie.

34. **Artikel 122** betreft de door operatoren bewaarde verkeers- en locatiegegevens in het kader van abonnees of eindgebruikers (§ 1), facturering (§ 2) , verwerking voor marketing (§ 3), fraude of kwaadwillig gebruik (§ 4), veiligheid en correcte werking communicatienetwerken- en diensten (§ 4/1), voldoen aan formeel wettelijke norm (§ 4/2), verwerking van die gegevens (§5).

Op basis van artikel 122 mogen of moeten volgende verkeers- en locatiegegevens door de operatoren bewaard worden: verkeersgegevens (bron, bestemming, datums, tijdstippen); locatie communicerende partijen; telefoonnummers, IP-adressen; gegevens specifiek geïdentificeerde fraude of kwaadwillig gebruik; gegevens nodig om veiligheid en correcte werking netwerken en diensten te garanderen.

In eerste instantie wordt gesteld dat ook de gegevens die door operatoren op zich mogen of moeten bewaard worden moeten beantwoorden aan de vereisten van de in het middel vermelde wettelijke bepalingen. Verzoeker stelt dat het – zoals hoger aangeduid – om een zeer breed geheel van verkeers- en locatiegegevens gaat. Het gaat om gegevens waarover de operator op zich beschikt in het kader van verkeer en locatie (§ 1). Het gaat ook over acht specifieke verkeersgegevens die verplicht bewaard worden teneinde maatregelen te nemen om fraude of kwaadwillig gebruik vast te stellen (§4, 1° en 2°). In dat kader kan de operator de verkeersgegevens doorsturen aan de bevoegde autoriteit. In dat kader kan een KB die verkeersgegevens nog preciseren en uitbreiden. (§4, 5°).

In tweede instantie stelt artikel 122, §4/2 dat de operatoren ook de verkeersgegevens bewaren en verwerken om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm. Artikel 122§5 stelt verder dat de verwerking van de gegevens die nodig zijn om te voldoen aan de verplichtingen van artikel 122, onder meer 'het voldoen aan de wettelijke verplichtingen', moet geschieden door personen in opdracht van de operator.

35. **Artikel 123** bepaalt dat de operatoren van mobiele netwerken andere locatiegegevens dan verkeersgegevens die betrekking hebben op een abonnee of eindgebruiker mogen bewaren en verwerken in geval het noodzakelijk is voor de goede werking en veiligheid van het netwerk of de dienst of om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren, en wanneer ze anoniem gemaakt zijn en wanneer de verwerking noodzakelijk is om te voldoen aan de verplichting van een formele wettelijke norm. In dit artikel is niet aangeduid om welke gegevens het dan precies gaat; er is enkel vermeld 'andere' locatiegegevens. In principe vallen hier alle locatiegegevens onder die niet onder artikel 122 vermeld zijn. Bij gebrek aan bepaling van die 'andere' gegevens gaat het om een breed gamma aan gegevens.

36. **Artikel 126** bepaalt dat de operatoren 17 met naam genoemde algemene (identificatie) gegevens moeten bewaren. Het gaat om het Rijksregisternummer; alias gebruiker; contactgegevens abonnee (e-mail en postadres); datum en tijdstip inschrijving (fysiek adres verkooppunt, fysiek adres netwerkaansluitpunt, IP-adres gediend voor inschrijving, geografische locatie eindapparatuur…); fysiek leveringsadres; facturatieadres, betalingswijze, betaalmiddel, tijdstip en referentie betaling in geval onlinebetaling; hoofddienst en aanvullende diensten gebruik abonnee; datum eerste gebruik en beëindiging; gegevens overdracht identifier abonnee (telefoonnummer, identiteit operator; toegewezen telefoonnummer; voornaamste e-mailadres en e-mailadressen alias; internationale identiteit IMSI (Intenational Mobile Subscriber Identity); permanent identifier abonnement SUPI (Subscription Permanent Identifier); verdoken indentifier van abonnement SUCI (Subscription Concealed Identifier); IP-adres bron verbinding, tijdstempel, eindgebruiker, poorten; Identifier eindapparatuur (IMEI adres; permanente identifier PEI (Permanent Equipment Identifier); adres controller (MAC)); andere identifiers met betrekking tot eindgebruiker, eindapparatuur.

Bij KB kunnen die gegevens gepreciseerd worden. Het gaat om een breed gamma van algemene gegevens die verplicht moeten bewaard worden door de operatoren. De gegevens moeten bewaard worden zolang de dienst gebruikt wordt en tot twaalf maanden na het einde van de dienst. In het artikel wordt niet vermeld met welk doel deze gegevens moeten bewaard worden.

37. **Artikel 126/1** bepaalt de gegevens die de operatoren moeten bewaren in het kader van de geografische zones bedoeld in artikel 126/3. Het gaat om tien gegevens vermeld in artikel 126/2 §2 (zie verder). Dit artikel bepaalt (wel) de doelstelling van de bewaring: vrijwaring nationale veiligheid, strijd tegen zware criminaliteit, preventie ernstige bedreiging van de openbare veiligheid, bescherming van de vitale belangen van een natuurlijk persoon. Het artikel bepaalt ook dat al de verkeersgegevens worden bewaard (ook oproepingen zonder resultaat) wanneer het ganse grondgebied als zone gedekt is door de bewaarplicht. Ook de gegevens met betrekking tot de verbinding van de eindapparatuur, inclusief netwerkaansluiting, wordt bewaard.

    Bij KB worden technische parameters voor gebruik gegevensopslag bepaald. Bij KB wordt een lijst van autoriteiten bepaald bevoegd voor aangelegenheden van artikel 126/3 §§ 2 tot 5. Bij KB worden in voorkomend geval bijkomende geografische zones bepaald.

38. **Artikel 126/2 § 2** bepaalt tien gegevens die de operatoren moeten bewaren in het kader van de geografische zones. Het zijn: de beschrijving en technische karakteristieken die werd aangewend tijdens de communicatie; bepaalde identificatiegegevens van de geadresseerde van de communicatie; het IP-adres van de geadresseerde, het tijdstempel…; identificatie van alle lijnen bij groepsgesprek of doorschakeling; datum en exacte tijdstip aanvang en einde sessie; gegevens identificatie en locatie van aansluitpunten communicatie, van start tot einde, en exacte data en tijdstippen locaties; het geüploade en gedownloade volume; datum en tijdstip verbinding van eindapparatuur met netwerk zowel opstart als uitschakeling; locatie eindapparatuur en datum en tijdstip locatie; andere identifiers met betrekking tot geadresseerde, tot zijn eindapparatuur.

    Bij KB kunnen vermelde gegevens gepreciseerd worden.

    Artikel 126/2 §3 stelt dat de combinatie van de gegevens die bewaard worden in uitvoering van artikel 126 en van artikel 126/2 het moet mogelijk maken om de relatie te leggen tussen de bron en de bestemming van de communicatie.

39. **Artikel 127** bepaalt een groot aantal gegevens die de operatoren moeten bewaren om de abonnees van een elektronische-communicatiedienst door middel van een directe of indirecte identificatiemethode te identificeren. In §6 van het artikel worden 32 toegestane identificatiedocumenten aangeduid. In §7 bepaalt dat van een abonnee met een Belgische elektronische identiteitskaart het rijksregisternummer, naam en voornaam worden bewaard; bij identificatie via ander document moeten zes gegevens worden bewaard. In § 10 is bepaald dat de operator de autoriteiten bedoeld in artikel 127/1 §3 het moet mogelijk maken om de abonnees via een indirecte identificatiemethode te identificeren. Het gaat om zes methodes zo onder meer de kenmerken van de betalingsverrichtingen.

C. <u>Het standpunt van het Hof van Justitie EU</u>

40. In het arrest SpaceNet AG maakt het HvJ met betrekking tot de bewaring van gegevens een onderscheid tussen algemeen bewaarde verkeers- en locatiegegevens en IP-adressen (eigen vetaanduidingen):

-overwegingen 76-94 in verband met algemene en ongedifferentieerde bewaring verkeers- en locatiegegeven;

-overwegingen 95-103 in verband met het bewaren van IP-adressen en identificatiegegevens.

Maatregel die voorziet in een algemene en ongedifferentieerde bewaring van het merendeel van de verkeers- en locatiegegevens voor een periode van meerdere weken

76 In het licht van deze principiële overwegingen moeten de door de verwijzende rechter onder de aandacht gebrachte kenmerken van de in de hoofdgedingen aan de orde zijnde nationale regeling worden onderzocht.

77 Wat in de eerste plaats de **omvang van de bewaarde gegevens** betreft, blijkt uit de verwijzingsbeslissing dat de bij die regeling opgelegde bewaringsverplichting bij de aanbieding van telefoondiensten onder **meer betrekking heeft op de gegevens die nodig zijn voor de identificatie van de bron en de bestemming van de communicatie, de datum en het tijdstip van het begin en het einde van de communicatie, of – bij verzending van een sms, een multimediabericht of een soortgelijk bericht – het tijdstip van de verzending en de ontvangst van het bericht en in het geval van mobiel gebruik de aanduiding van de aan het begin van de communicatie door de oproeper en de opgeroepene gebruikte netwerkcellen. Bij de aanbieding van internettoegangsdiensten heeft de bewaringsverplichting onder meer betrekking op het aan de abonnee toegewezen IP-adres, de datum en het tijdstip van het begin en het einde van het internetgebruik via het toegewezen IP-adres en in het geval van mobiel gebruik de aanduiding van de bij het begin van de internetverbinding gebruikte netwerkcellen. Ook worden de gegevens bewaard op basis waarvan de geografische locatie en de hoofdstraalrichtingen van de netwerkantennen die de betreffende netwerkcel bedienen, kunnen worden bepaald.**

78 Ofschoon de bewaringsverplichting volgens de in de hoofdgedingen aan de orde zijnde nationale regeling **niet ziet op de inhoud** van de communicatie en op de gegevens die betrekking hebben op de bezochte websites, en ofschoon die regeling de bewaring van de netwerkcelidentificator slechts verplicht stelt bij het begin van de communicatie, dient te worden opgemerkt dat dit in wezen ook het geval was bij de nationale regelingen tot omzetting van richtlijn 2006/24 die aan de orde waren in de zaken die hebben geleid tot het arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791). **Ondanks deze beperkingen heeft het Hof in dat arrest geoordeeld dat het op basis van de categorieën van gegevens die op grond van die richtlijn en van de betreffende nationale regelingen werden bewaard, mogelijk was om zeer precieze conclusies te trekken over het privéleven van de betrokken personen, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren, en met name om het profiel van de betrokken personen op te stellen.**

79 Bovendien dient te worden vastgesteld dat de in de hoofdgedingen aan de orde zijnde regeling weliswaar niet ziet op gegevens die betrekking hebben op de bezochte websites, maar dat zij niettemin voorschrijft dat **de IP-adressen worden bewaard**. IP-adressen kunnen onder meer

worden gebruikt om op exhaustieve wijze te traceren welke websites een internetgebruiker heeft bezocht en bijgevolg wat zijn onlineactiviteiten zijn, zodat aan de hand van die gegevens het gedetailleerde profiel van de betrokkene kan worden opgesteld. De voor een dergelijke tracking noodzakelijke bewaring en analyse van die IP-adressen vormen dan ook **ernstige inmengingen** in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van de internetgebruiker (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 153).

80 Bovendien vallen de gegevens betreffende e-maildiensten weliswaar niet onder de bewaringsverplichting die wordt opgelegd bij de in de hoofdgedingen aan de orde zijnde regeling, maar vormen zij – zoals SpaceNet in haar schriftelijke opmerkingen heeft opgemerkt – slechts een zeer klein deel van de gegevens in kwestie.

81 Zoals de advocaat-generaal in wezen heeft opgemerkt in punt 60 van zijn conclusie, strekt de bewaringsverplichting die is neergelegd in de nationale regeling die in de hoofdgedingen aan de orde is, zich dan ook uit tot **een zeer breed scala aan verkeers- en locatiegegevens**, dat in essentie overeenkomt met die welke hebben geleid tot de in punt 78 van dit arrest in herinnering gebrachte rechtspraak.

82 Bovendien heeft de Duitse regering in antwoord op een ter terechtzitting gestelde vraag gepreciseerd dat slechts **1 300 entiteiten waren opgenomen op de lijst van personen, instanties of organisaties van sociale of godsdienstige aard** waarvan de gegevens over elektronische communicatie op grond van § 99, lid 2, en § 113b, lid 6, TKG **niet worden bewaard**, hetgeen onmiskenbaar een **beperkt aantal** is ten opzichte van alle gebruikers van telecommunicatiediensten in Duitsland van wie de gegevens wel vallen onder de bewaringsverplichting die wordt opgelegd bij de in de hoofdgedingen aan de orde zijnde nationale regeling. Zo worden onder meer de gegevens van aan het beroepsgeheim onderworpen gebruikers, zoals advocaten, artsen en journalisten, bewaard.

83 Uit de verwijzingsbeslissing blijkt dus dat de door deze nationale regeling **voorgeschreven bewaring van verkeers- en locatiegegevens betrekking heeft op nagenoeg de hele bevolking, zonder dat de betrokkenen zich – al was het maar indirect – in een situatie bevinden die aanleiding kan geven tot strafrechtelijke vervolging**. Evenzo stelt die **regeling de algemene en vanuit een persoonlijk, temporeel en geografisch oogpunt ongedifferentieerde bewaring – zonder grondslag – van het merendeel van de verkeers- en locatiegegevens verplicht,** waarvan de omvang in wezen overeenkomt met die van de gegevens die werden bewaard in de zaken die hebben geleid tot de in punt 78 van dit arrest aangehaalde rechtspraak.

84 Gelet op de rechtspraak die in punt 75 van dit arrest is aangehaald, kan een verplichting tot bewaring van gegevens zoals die welke in de hoofdgedingen aan de orde is – anders dan de Duitse regering stelt – dan ook **niet worden beschouwd als een gerichte bewaring van gegevens.**

85 Wat in de **tweede plaats** de duur van de gegevensbewaring betreft, volgt uit artikel 15, lid 1, tweede volzin, van richtlijn 2002/58 dat de **bewaarperiode** die is vastgesteld in een nationale maatregel waarbij een algemene en ongedifferentieerde bewaringsverplichting wordt opgelegd,

een van de relevante factoren is om te bepalen of het Unierecht zich tegen die maatregel verzet, aangezien voornoemde volzin vereist dat deze **periode „beperkt"** is.

86 In casu is het juist dat de duur van de bewaarperioden, die volgens § 113b, lid 1, TKG maximaal **vier weken** bedraagt voor locatiegegevens en maximaal **tien weken** voor de overige gegevens, aanzienlijk korter is dan de duur van de perioden in de door het Hof in zijn arresten van 21 december 2016, Tele2 Sverige en Watson e.a. (C-203/15 en C-698/15, EU:C:2016:970), 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791), en 5 april 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258), onderzochte nationale regelingen waarbij een algemene en ongedifferentieerde bewaringsverplichting werd opgelegd.

87 Zoals blijkt uit de in punt 61 van het onderhavige arrest aangehaalde rechtspraak, **vloeit de ernst van de inmenging echter voort uit het risico dat de bewaarde gegevens – met name gelet op de talrijkheid en de verscheidenheid ervan – het in hun geheel beschouwd mogelijk maken om zeer precieze conclusies te trekken over het privéleven van de persoon of personen van wie de gegevens zijn bewaard, en dat aan de hand van die gegevens in het bijzonder het profiel van de betrokken persoon of personen kan worden opgesteld, informatie die vanuit het oogpunt van het recht op eerbiediging van het privéleven even gevoelige informatie is als de inhoud zelf van de communicatie.**

88 Derhalve vormt de bewaring van verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicatie van een gebruiker van een elektronische-communicatiemiddel of over de locatie van de door hem gebruikte eindapparatuur, **hoe dan ook een ernstige inmenging, ongeacht de duur van de bewaarperiode, de hoeveelheid of de aard van de bewaarde gegevens,** wanneer op basis van die gegevens als geheel precieze conclusies kunnen worden getrokken over het privéleven van de betrokken persoon of personen [zie, met betrekking tot de toegang tot dergelijke gegevens, arrest van 2 maart 2021, Prokuratuur (Voorwaarden voor toegang tot elektronische-communicatiegegevens), C-746/18, EU:C:2021:152, punt 39].

89 In dit verband kan **zelfs de bewaring van een beperkte hoeveelheid verkeers- of locatiegegevens of de bewaring van deze gegevens voor een korte periode zeer precieze informatie over het privéleven van een gebruiker van een elektronische-communicatiemiddel verschaffen.** Bovendien kunnen de hoeveelheid beschikbare gegevens en de daaruit voortvloeiende zeer precieze informatie over het privéleven van de betrokkene pas na inzage van deze gegevens worden beoordeeld. De inmenging die het gevolg is van de bewaring van die gegevens, vindt echter noodzakelijkerwijs plaats voordat de gegevens en de daaruit voortvloeiende informatie kunnen worden geraadpleegd. De ernst van de inmenging die de bewaring met zich meebrengt voor het privéleven van de betrokken personen, wordt dus noodzakelijkerwijs beoordeeld op basis van het risico dat in het algemeen verbonden is aan de categorie van bewaarde gegevens, waarbij het niet van belang is of de daaruit voortvloeiende informatie over het privéleven concreet gesproken al dan niet gevoelig is [zie in die zin arrest van 2 maart 2021, Prokuratuur (Voorwaarden voor toegang tot elektronische-communicatiegegevens), C-746/18, EU:C:2021:152, punt 40].

90 Zoals blijkt uit punt 77 van het onderhavige arrest en zoals ter terechtzitting is bevestigd, kunnen in casu op basis van een geheel van verkeers- en locatiegegevens die gedurende respectievelijk tien en vier weken worden bewaard, zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren, en kan aan de hand van deze gegevens met name een profiel van die personen worden opgesteld.

91 Wat in de **derde plaats de waarborgen** betreft waarin de in de hoofdgedingen aan de orde zijnde nationale regeling voorziet en die ertoe strekken de bewaarde gegevens te **beschermen tegen de risico's op misbruik en tegen elke onrechtmatige toegang,** zij opgemerkt dat de **bewaring van deze gegevens en de toegang** ertoe – zoals blijkt uit de in punt 60 van het onderhavige arrest in herinnering gebrachte rechtspraak – **onderscheiden inmengingen** in de door de artikelen 7 en 11 van het Handvest gewaarborgde grondrechten vormen waarvoor een **verschillende rechtvaardiging vereist** is op grond van artikel 52, lid 1, van het Handvest. Derhalve kan een nationale wettelijke regeling die zorgt voor de volledige naleving van de voorwaarden die voortvloeien uit de rechtspraak waarbij richtlijn 2002/58 is uitgelegd op het gebied van de toegang tot de bewaarde gegevens, per definitie de ernstige inmenging in de door de artikelen 5 en 6 van deze richtlijn gewaarborgde rechten en in de grondrechten waarvan deze artikelen de concretisering vormen, beperken noch verhelpen (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 47).

92 Wat in de **vierde en laatste plaats** het **argument van de Europese Commissie** betreft dat **bijzonder zware criminaliteit kan worden gelijkgesteld met een bedreiging voor de nationale veiligheid**, heeft het Hof reeds geoordeeld dat de **doelstelling de nationale veiligheid te beschermen strookt met het eminente belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving door het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en met name een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 61 en aldaar aangehaalde rechtspraak).

93 In tegenstelling tot – zelfs zeer zware – criminaliteit moet een **bedreiging voor de nationale veiligheid reëel en actueel of op zijn minst voorzienbaar zijn** – wat onderstelt dat zich voldoende concrete omstandigheden voordoen – om een rechtvaardiging te kunnen vormen voor een maatregel die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens gedurende een beperkte periode. Door de aard van een dergelijke bedreiging, haar ernst en het specifieke karakter van de omstandigheden waarin zij zich voordoet, **onderscheidt zij zich van het algemene en permanente risico dat er – zelfs ernstige – spanningen of wanordelijkheden plaatsvinden die de openbare veiligheid ondermijnen of dat er ernstige strafbare feiten worden gepleegd** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 62 en aldaar aangehaalde rechtspraak).

94 Derhalve **kan – zelfs zeer zware – criminaliteit niet worden gelijkgesteld met een bedreiging voor de nationale veiligheid.** Met een dergelijke gelijkstelling zou namelijk een categorie tussen nationale veiligheid en openbare veiligheid in kunnen worden gecreëerd om vervolgens op laatstgenoemde categorie de vereisten toe te passen die inherent zijn aan eerstgenoemde categorie (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 63).

Maatregelen die voorzien in (een gerichte bewaring, een spoedbewaring of) een bewaring van IP-adressen

95 Meerdere regeringen, waaronder de Franse, benadrukken dat enkel een algemene en ongedifferentieerde bewaring het mogelijk maakt om de met de bewaringsmaatregelen nagestreefde doelstellingen op doeltreffende wijze te verwezenlijken, waarbij de Duitse regering in wezen preciseert dat aan deze gevolgtrekking niet wordt afgedaan door het feit dat de lidstaten kunnen gebruikmaken van de in punt 75 van het onderhavige arrest bedoelde maatregelen die voorzien in gerichte bewaring en spoedbewaring.

96 Dienaangaande zij in de **eerste plaats** opgemerkt dat de **doeltreffendheid van strafvervolging doorgaans niet afhangt van één onderzoeksmiddel, maar van alle onderzoeksmiddelen waarover de bevoegde nationale autoriteiten te dien einde beschikken** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 69).

97 In de **tweede plaats** is het de lidstaten krachtens artikel 15, lid 1, van richtlijn 2002/58 – gelezen in het licht van de artikelen 7, 8 en 11 alsook artikel 52, lid 1, van het Handvest, zoals uitgelegd in de in punt 75 van het onderhavige arrest in herinnering gebrachte rechtspraak – **toegestaan om ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen voor de openbare veiligheid** niet alleen maatregelen te treffen die voorzien in **gerichte bewaring en spoedbewaring,** maar **ook** maatregelen die voorzien in een **algemene en ongedifferentieerde bewaring** van ten eerste de gegevens die betrekking hebben op de **burgerlijke identiteit** van gebruikers van elektronische-communicatiemiddelen, en ten tweede de **IP-adressen** die zijn toegewezen aan de bron van een verbinding (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 70).

98 In zoverre staat het vast dat de bewaring van gegevens betreffende de burgerlijke identiteit van gebruikers van elektronische-communicatiemiddelen kan bijdragen tot de bestrijding van zware criminaliteit, voor zover het aan de hand van deze gegevens mogelijk is om de personen te identificeren die zich van die middelen hebben bediend bij de voorbereiding of het plegen van een daad die onder zware criminaliteit valt (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 71).

99 Richtlijn 2002/58 staat niet in de weg aan de algemene bewaring – met het oog op de bestrijding van criminaliteit in het algemeen – van gegevens die betrekking hebben op de burgerlijke identiteit. Gepreciseerd moet dan ook worden dat deze richtlijn, noch enige andere Unierechtelijke handeling zich verzet tegen een nationale wettelijke regeling die tot doel heeft zware criminaliteit te bestrijden, op grond waarvan de **aankoop van een elektronische-communicatiemiddel** – zoals een prepaid simkaart – afhankelijk wordt gesteld van de **verificatie**

van officiële documenten waaruit de identiteit van de koper blijkt, alsmede van de registratie door de verkoper van de daaruit voortvloeiende informatie, waarbij de verkoper in voorkomend geval gehouden is om de bevoegde nationale autoriteiten toegang tot deze informatie te verlenen (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 72).

100 Voorts zij eraan herinnerd dat de **algemene bewaring van de IP-adressen** van de bron van de verbinding op ernstige wijze inbreuk maakt op de in de artikelen 7 en 8 van het Handvest neergelegde grondrechten – aangezien op basis van die IP-adressen precieze conclusies kunnen worden getrokken over het privéleven van de gebruiker van het betreffende elektronische-communicatiemiddel – en een **ontradend effect kan hebben op de gebruikmaking van de door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting**. Het Hof heeft in verband met die bewaring echter vastgesteld dat de verzoening van de rechten en legitieme belangen in kwestie, die noodzakelijk is volgens de rechtspraak die is vermeld in de punten 65 tot en met 68 van het onderhavige arrest, vereist dat in aanmerking wordt genomen dat in het geval van een online gepleegd strafbaar feit, en met name in het geval van het **online verwerven, verspreiden, uitzenden of ter beschikking stellen van kinderpornografie** in de zin van artikel 2, onder c), van richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van kaderbesluit 2004/68/JBZ van de Raad (PB 2011, L 335, blz. 1; met rectificatie in PB 2012, L 18, blz. 7), het IP-adres mogelijkerwijs het enige onderzoeksmiddel is dat het mogelijk maakt om de persoon te identificeren aan wie dat adres was toegewezen toen dat feit werd gepleegd (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 73).

101 Dat een wettelijke maatregel die voorziet in de bewaring van de IP-adressen van alle natuurlijke personen die eigenaar zijn van eindapparatuur waarmee internettoegang kan worden verkregen, personen betreft bij wie er op het eerste gezicht geen sprake is van een verband – in de zin van de in punt 70 van het onderhavige arrest aangehaalde rechtspraak – met de nagestreefde doelstellingen, en dat internetgebruikers, zoals in punt 54 van dit arrest is vastgesteld, er krachtens de artikelen 7 en 8 van het Handvest op mogen vertrouwen dat hun identiteit in beginsel niet wordt onthuld, neemt dan ook niet weg dat een wettelijke maatregel die voorziet in de algemene en **ongedifferentieerde bewaring van uitsluitend de aan de bron van een verbinding toegewezen IP-adressen**, in beginsel **niet in strijd is met artikel 15, lid 1**, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 alsook artikel 52, lid 1, van het Handvest, **mits** deze mogelijkheid afhankelijk wordt gesteld van de strikte naleving van de **materiële en procedurele voorwaarden die het gebruik** van die gegevens behoren te regelen (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 155).

102 Gelet op de met die bewaring gepaard gaande ernstige inmenging in de grondrechten die worden erkend in de artikelen 7 en 8 van het Handvest, kunnen – **behalve de bescherming van de nationale veiligheid – enkel de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid die inmenging rechtvaardigen.** Bovendien mag de **bewaarperiode niet langer duren dan strikt noodzakelijk is voor de nagestreefde**

doelstelling. Ten slotte moet een maatregel van deze aard voorzien in **strikte voorwaarden en waarborgen** met betrekking tot het gebruik dat van de gegevens in kwestie wordt gemaakt, met name in de vorm van het in kaart brengen van de onlinecommunicatie en de onlineactiviteiten van de betrokken personen (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 156).

103 Anders dan de verwijzende rechter heeft benadrukt, staan de punten 155 en 168 van het arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791), onderling dus niet op gespannen voet. Zoals de advocaat-generaal in de punten 81 en 82 van zijn conclusie in wezen heeft opgemerkt, komt uit voornoemd punt 155, gelezen in samenhang met de punten 156 en 168 van dat arrest, namelijk duidelijk naar voren dat behalve de bescherming van de nationale veiligheid **enkel de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen voor de openbare veiligheid een rechtvaardiging kunnen vormen voor de algemene bewaring van de IP-adressen** die zijn toegewezen aan de bron van een verbinding, ongeacht of er – op zijn minst indirect – sprake is van een verband tussen de betrokken personen en de nagestreefde doelstellingen.

D. Systematisering standpunt Hof van Justitie EU

41. Wat het TKG betreft, stelt het Hof vast dat uit de verwijzingsbeslissing blijkt dat de bij deze wet opgelegde bewaringsverplichting onder meer betrekking heeft op de gegevens die nodig zijn voor de **identificatie van de bron en de bestemming van de communicatie, de datum en het tijdstip van het begin en het einde van de communicatie, of – bij verzending van een sms, een multimediabericht of een soortgelijk bericht – het tijdstip van de verzending en de ontvangst van het bericht en in het geval van mobiel gebruik de aanduiding van de aan het begin van de communicatie door de oproeper en de opgeroepene gebruikte netwerkcellen.**

Bij de aanbieding van internettoegangsdiensten heeft de bewaringsverplichting onder meer betrekking op het aan **de abonnee toegewezen IP-adres, de datum en het tijdstip van het begin en het einde van het internetgebruik via het toegewezen IP-adres en in het geval van mobiel gebruik de aanduiding van de bij het begin van de internetverbinding gebruikte netwerkcellen. Ook de gegevens op basis waarvan de geografische locatie en de hoofdstraalrichtingen van de netwerkantennes die de betreffende netwerkcel** bedienen kunnen worden bepaald, worden bewaard.

De gegevens betreffende e-maildiensten vallen weliswaar niet onder de bij het TKG opgelegde bewaringsverplichting, maar vormen slechts een uiterst klein deel van de gegevens in kwestie. Voorts worden onder meer de **gegevens van aan het beroepsgeheim onderworpen gebruikers, zoals advocaten, artsen en journalisten, bewaard.**

De in het TKG neergelegde bewaringsverplichting strekt zich dan ook uit tot een **zeer breed geheel van verkeers- en locatiegegevens,** dat in essentie overeenkomt met die welke hebben geleid tot de eerdere arresten die hierboven zijn genoemd.

Op basis van dat geheel van verkeers- en locatiegegevens die gedurende respectievelijk tien en vier weken worden bewaard, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard – zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren – en kan met name een profiel van die personen worden opgesteld.

De burgerlijke gegevens en IP-adressen kunnen onder bepaalde voorwaarden algemeen en ongedifferentieerd bewaard worden.

E. Discussie en toepassing

42. De door de operatoren te bewaren gegevens moeten op zich beoordeeld worden én ook in het kader van de voorwaarden en gevallen waarin zij verplicht moeten bewaard worden.

43. *Geen bewaring van de inhoud van de communicatie*

Op basis van het groot aantal te bewaren gegevens en op basis van de categorieën van gegevens die moeten bewaard worden, is het mogelijk om zeer precieze conclusies te trekken over het privéleven van de betrokken personen, zoals de dagelijkse gewoonten, hun permanente of tijdelijke verblijfsplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren, en om een profiel van de betrokken personen op te stellen. (SpaceNet, 78). De voorliggende wet legt de mogelijkheid en/of verplichting op aan de operatoren om én een groot aantal (ongeveer 60) én diverse categorieën (verkeers-, locatie-, identificatie data) gegevens te bewaren. Dit gegeven op zich maakt dat artikel 22 Grondwet en artikels 7 en 8 Handvest geschonden worden, daar zo het persoonlijk leven van de burgers niet langer beschermde is.

44. Wat betreft de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens.

45. In de zaak TKG stelt het HvJ dat artikel 15, lid 1 richtlijn 2002/58/EG in het licht van artikelen 7, 8 en 11 alsook artikel 52, lid 1 van het Handvest, zich verzetten tegen de bewaringsplicht die zich uitstrekt tot een zeer breed geheel van verkeers- en locatiegegevens op zich en dus los van de voorwaarden en de situaties waarin deze moeten bewaard worden. (SpaceNet AG, punt 81)

De artikels 122, 123, 126, 126/1, 126/2 en 127 ingevoerd door de wet van 20 juli 2022 bepalen dat de operatoren een massale hoeveelheid gegevens mogen en/of moeten bewaren. Het gaat om een zeer breed geheel van identiteits-, verkeers- en locatiegegevens. Deze hoger gesystematiseerde gegevens worden hier als herhaald aanzien. Het gaat om een zestigtal onderscheiden gegevens.

Het gaat onbetwistbaar over een nog breder geheel aan gegevens dan wat in de TKG was bepaald en door het HvJ werd afgewezen. Ook de in de TKG bepaalde korte bewaarperiode (vier tot tien weken) en de bepaling dat 1.300 entiteiten opgenomen waren op een lijst waarvan de gegevens over de elektronische communicatie niet werden bewaard (SpaceNet, punt 82) zijn voor het HvJ niet afdoende om de bewaringsplicht te rechtvaardigen. In de hier bestreden wet wordt overigens voorzien in langere

bewaringstermijnen en zijn er geen entiteiten (ook niet artsen, advocaten en journalisten) van wie de gegevens niet bewaard mogen worden.

46. Wat de omvang van de door vermelde artikels van de wet van 20 juli 2022 bewaarde gegevens betreft, blijkt dat de aan de operatoren opgelegde bewaringsverplichting onder meer betrekking heeft op de gegevens die nodig zijn voor de identificatie van de bron en de bestemming van de communicatie, de datum en het tijdstip van het begin en het einde van de communicatie, of – bij verzending van een sms, een multimediabericht of een soortgelijk bericht – het tijdstip van de verzending en de ontvangst van het bericht en in het geval van mobiel gebruik de aanduiding van de aan het begin van de communicatie door de oproeper en de opgeroepene gebruikte netwerkcellen. Bij de aanbieding van internettoegangsdiensten heeft de bewaringsverplichting onder meer betrekking op het aan de abonnee toegewezen IP-adres, de datum en het tijdstip van het begin en het einde van het internetgebruik via het toegewezen IP-adres en in het geval van mobiel gebruik de aanduiding van de bij het begin van de internetverbinding gebruikte netwerkcellen. Ook worden de gegevens bewaard op basis waarvan de geografische locatie en de hoofdstraalrichtingen van de netwerkantennen die de betreffende netwerkcel bedienen, kunnen worden bepaald. (SpaceNet AG, punt 77).

47. De in de wet van 20 juli 2022 voorgeschreven bewaring van verkeers- en locatiegegevens heeft betrekking op nagenoeg de hele bevolking, zonder dat de betrokkenen, ook niet indirect, zich in een situatie bevinden die aanleiding geeft tot strafrechtelijke vervolging. De regeling stelt een algemene en vanuit persoonlijk, temporeel en geografisch oogpunt ongedifferentieerde bewaring – zonder grondslag – van het merendeel van de verkeers- en locatiegegevens verplicht. (SpaceNet AG, punt 82).

    In dit kader wordt gesteld dat de grondslag van de bewaring niet is opgenomen in de artikels 126 waarbij de operatoren verplicht worden een uitgebreide lijst van 17 gegevens te bewaren. In de artikels 122 en 123 is de doelstelling wel opgenomen (abonnees, facturering, marketing, veiligheid netwerk, kwaadwillig gebruik of fraude netwerk). Maar ook deze gegevens kunnen door de autoriteiten die toegang hebben onder bepaalde voorwaarden, die niets te maken hebben met vermelde doelstelling, opgevraagd worden. In artikel 126/1 § 2 is met betrekking tot bewaring in geografische zones als doelstelling de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, preventie ernstige dreiging van openbare veiligheid, en bescherming vitale belangen van een natuurlijk persoon, opgenomen. Evenwel bepaalt artikel 126/1 § 5 dat geografische zones enkel kunnen opgenomen worden ter vrijwaring van de nationale veiligheid of hoog risico op zware criminaliteit. De 'grondslagen' spreken elkaar tegen. Er zal in het tweede onderdeel geargumenteerd worden dat ook de bewaring in geografische zones zoals door de wet van 20 juli 2022 bepaald, de facto een algemene en ongedifferentieerde bewaring creëert. Overigens stelt de wet in artikel 126/1 § 3, alinea 2 dat in het kader van artikel 126/3 (zonder onderscheid in de vijf criteria van dit artikel) de bewaarplicht het ganse grondgebied kan dekken.

48. De GBA merkt bovendien op dat "*het voorontwerp van wet, door een nieuwe veralgemeende bewaarplicht voor verkeers- en locatiegegevens op te leggen met het oog op de bestrijding van fraude en kwaadwillig gebruik van het netwerk, en er tegelijkertijd voor te zorgen dat (onder meer) wetshandhavingsinstanties toegang hebben tot dergelijke gegevens, de facto leidt tot de herinvoering van een veralgemeende en ongedifferentieerde bewaarplicht voor dergelijke gegevens met het oog op de bestrijding van criminaliteit*" (Advies GBA, Parl. St., Kamer, Doc 55 2572/001, p. 752).

Daarenboven vraagt de GBA zich ook af "*of een verplichting tot preventieve en systematische gegevensbewaring, zoals is voorzien in het nieuwe artikel 122 § 4 van de telecomwet, noodzakelijk is om een vermoed geval van fraude of een vermoed geval van kwaadwillig gebruik van het elektronische communicatienetwerk op te sporen en te analyseren*" (Advies GBA, Parl. St., Kamer, Doc 55 2572/001, p. 752).

49. Dezelfde vragen en opmerkingen worden ook gesteld betreffende (i) de verplichting om systematisch de verkeersgegevens te bewaren van alle gebruikers van de elektronische communicatiemiddelen en (ii) de mogelijkheid tot verwerking van andere locatiegegevens dan verkeersgegevens om de correcte werking en de veiligheid van het netwerk of de dienst te garanderen of om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren.

    De drie artikels 123, 126, 126/1 stellen dat zij gelden 'onverminderd de AVG en de wet van 30 juli 2018'. Deze bepaling is indicatief. Het is evident dat de AVG en de wet van 30 juli 2018 gelden. Het punt is dat de wet van 20 juli 2022 zelf de bepalingen van de AVG en de wet van 30 juli 2018, moet respecteren. Het volstaat niet dat de wet van 20 juli 2022 vermelde bepaling opneemt om zo het respect voor die bepalingen te rechtvaardigen.

50. De bewaringsverplichting ziet niet toe op de inhoud van de communicatie. Dit was ook in wezen het geval bij de nationale – onder meer Belgische – regelingen tot omzetting van richtlijn 2006/24 die aan de orde waren in de zaken die hebben geleid tot het arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791). Ondanks deze beperkingen heeft het Hof in dat arrest geoordeeld dat het op basis van de categorieën van gegevens die op grond van die richtlijn en van de betreffende nationale regelingen werden bewaard, mogelijk was om zeer precieze conclusies te trekken over het privéleven van de betrokken personen, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren, en met name om het profiel van de betrokken personen op te stellen. (SpaceNet AG, punt 78).

51. Specifiek wat betreft de algemene en ongedifferentieerde bewaring van gegevens die betrekking hebben op de burgerlijke identiteit van gebruikers en van IP-adressen.

52. Dit is toegestaan voor de bescherming van de nationale veiligheid, en enkel ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen voor de openbare veiligheid. (SpaceNet, 97, 102). Het HvJ situeert de bewaring van IP-adressen inzonderheid in het bestrijden van het verspreiden, verwerven, uitzenden of ter beschikking stellen van kinderporno en ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen, waarbij het IP-adres 'mogelijk het enige onderzoeksmiddel' is. (SpaceNet, 100) Het HvJ wijst er op dat deze bewaring een ontradend effect kan hebben op de gebruikmaking van het door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting. (SpaceNet, 100) Het HvJ stelt dan ook dat die bewaring kan 'mits deze mogelijkheid afhankelijk wordt gesteld van de strikte naleving van de materiële en procedurele voorwaarden die het gebruik regelen (SpaceNet, 101), dat de bewaarperiode niet langer duurt dan strikt noodzakelijk voor de nagestreefde doelstelling, en dat de maatregel voorziet in strikte voorwaarden en waarborgen met betrekking tot het gebruik van de gegevens. (SpaceNet, 102)

53. De wettelijke regeling in de hier besteden wet van 20 juli 2022 is complex wat betreft de bewaring van burgerlijke identiteit en IP-adressen.

Artikel 122§4 legt de operatoren de bewaring op van de identifier van de bron van de communicatie en van het IP-adres van de verzender van de communicatie, in het kader van fraude of kwaadwillig gebruik van het netwerk. Artikel 126 §1 legt in het algemeen de verplichting op tot bewaren van rijksregisternummer, identifier-gegevens en IP-adres bij inschrijving of activering. Er wordt in het artikel niet vermeld welke het kader is waarin deze gegevens moeten bewaard worden. Deze (en diverse andere) gegevens worden bewaard tot twaalf maanden na het einde van de dienst. Artikel 126/1 stelt dat voor de geografische zones de gegevens vermeld in artikel 126/2§ 2 (waar onder §2, 2°, identificatiegegevens en §2,3° IP-adres) bewaard worden. Enkel in dit artikel 126/1§1, derde alinea is bepaald dat de doelstelling in dit kader is de vrijwaring van de nationale veiligheid, de strijd tegen de zware criminaliteit, de preventie van ernstige bedreiging van de openbare veiligheid en de bescherming van de vitale belangen van een natuurlijke persoon. Artikel 127 legt de bewaring op van een grote reeks identificatiegegevens; in §6 gaat het om 32 gegevens.

Vermelde artikels beantwoorden wat betreft de bewaring van burgerlijke identiteit en IP-adres niet aan de voorwaarden zoals bepaald in het arrest SpaceNet van het HvJ. Het kader van de bewaring is veel ruimer dan enkel nationale veiligheid, zware criminaliteit en voorkoming ernstige bedreiging openbare veiligheid. In de artikels is ofwel geen grondslag of kader bepaald waarvoor die gegevens moeten of mogen bewaard worden, ofwel is de grondslag voor de bewaring de veiligheid van het netwerk of de bescherming van vitale belangen van een natuurlijke persoon. Enkel in artikel 126/1 §1 is het kader bepaald. Er zijn verder geen materiële en procedurele voorwaarden bepaald die het gebruik regelen, ook niet in het kader van artikel 126/1. . Er zijn evenmin strikte voorwaarden en waarborgen bepaald met betrekking tot het gebruik van de gegevens.

54. Om vermelde redenen zijn de artikels 122, 123, 126, 126/1 en 126/2 ingevoegd door de wet van 20 juli 2022 in de wet van 13 juni 2005, in strijd met de in het middel aangehaalde bepalingen en dienen zij vernietigd te worden.

VI.3. DERDE MIDDEL

Geschonden wetsartikels en referentienormen

Schending van artikel 11, 12, 22 en 29 Grondwet.

Schending van artikel 15, lid 1 en de artikels 5, 6 en 9 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), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

Schending van artikel 6, 8, 10, 11 en 18 van het Europees Verdrag voor de bescherming van de Rechten van de Mens (EVRM).

Schending van de artikels 13 en 54 van de Richtlijn 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Geschonden referentienormen.

Recht op eerbiediging van de persoonlijke levenssfeer en bescherming van persoonlijke data, al dan niet in samenhang gelezen met het recht op vertrouwelijkheid van communicatie en met de algemene beginselen van informatieve zelfbeschikking en de beginselen van noodzaak in een democratische samenleving, legaliteit, proportionaliteit en subsidiariteit.

De schending van de in het middel vermelde wettelijke bepalingen door artikel 126/3, ingevoegd of gewijzigd door de artikel 11 van de wet van 20 juli 2022 in de wet van 13 juni 2005 betreffende elektronische communicatie, inhoudend de bepalingen met betrekking tot de <u>geografische zones</u> waarin de gegevens bepaald in artikel 126/2 §2 moeten bewaard worden, en door artikel 45 alinea 1 van de wet van 20 juli 2022 betreffende het verzamelen en bewaren van de identiteitsgegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten. De diversiteit en omvang van de geografische zones voert de iure en de facto een algemene en ongedifferentieerde opslag van gegevens in.

A. <u>Aangevochten wettelijke bepalingen</u>

55. **Art. 126/2. § 1. …**

§ 2. De gegevens bedoeld in artikel 126/1, § 2, die in uitvoering van de artikelen 126/1 en 126/3 bewaard moeten worden door de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook door de operatoren die de onderliggende elektronische-communicatienetwerken aanbieden die het aanbieden van die diensten mogelijk maken, zijn de volgende:

1° de beschrijving en de technische karakteristieken van de elektronische-communicatiedienst die werd aangewend tijdens de communicatie;

2° de identificatiegegevens bedoeld in artikel 126, § 1, 2°, 10° tot 14°, en 16°, van de geadresseerde van de communicatie;

3° voor de elektronische-communicatiediensten met uitzondering van de internettoegangsdiensten, het IP-adres dat gebruikt is door de geadresseerde van de communicatie, het tijdstempel alsook, in geval van gedeeld gebruik van een IP-adres van de geadresseerde, de poorten die aan hem zijn toegewezen;

4° in geval van een groepsgesprek, oproepdoorschakeling of -doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;

5° de datum en het exacte tijdstip van de aanvang en het einde van de sessie van de betrokken elektronische-communicatiedienst, waaronder de datum en het exacte tijdstip van de aanvang en het einde van de oproep;

6° de gegevens die de identificatie en de lokalisatie van de cellen of andere netwerkaansluitpunten van het mobiele netwerk mogelijk maken, die werden gebruikt voor de communicatie, van de start tot het einde van de communicatie, alsook de exacte data en tijdstippen van deze verschillende locaties;

7° het tijdens de duur van de sessie geüploade en gedownloade volume van gegevens;

8° voor wat betreft de mobiele elektronische-communicatiediensten, de datum en het tijdstip van de verbinding van de eindapparatuur met het netwerk wegens het opstarten van die apparatuur, en het moment waarop de verbinding van deze eindapparatuur met het netwerk wordt verbroken wegens het uitschakelen van die apparatuur;

9° voor wat betreft de mobiele elektronische-communicatiediensten, de locatie van de eindapparatuur en de datum en het tijdstip van deze locatie telkens wanneer de operator wil weten welke eindapparatuur is verbonden met zijn netwerk;

10° de andere identifiers met betrekking tot de geadresseerde van de elektronische communicatie, tot zijn eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning bepaald worden, na advies van de Gegevensbeschermingsautoriteit en het Instituut, op voorwaarde dat dit besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

In afwijking van de artikelen 126/1 en 126/3 bedraagt de bewaartermijn van het gegeven bedoeld in het eerste lid, 8°, zes maanden nadat het is gegenereerd of verwerkt.

Het koninklijk besluit bedoeld in het eerste lid, 10°, slaat niet op de inhoud van de elektronische communicatie.

De Koning kan, na advies van de Gegevens-beschermingsautoriteit en het Instituut, de gegevens bedoeld in eerste lid, preciseren.

Art. 126/3. § 1. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones bestaande uit:

- de gerechtelijke arrondissementen waar minstens drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren;

- de politiezones waar minstens drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, en die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, eerste streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:

a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:

a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

Het aldus vastgestelde aantal strafbare feiten wordt naar boven of naar beneden afgerond op het dichtstbijzijnde gehele getal, al naargelang het eerste cijfer achter de komma al dan niet vijf bereikt.

De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld over een gemiddelde van de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet van 5 augustus 1992 op het politieambt.

De grenzen van de gerechtelijke arrondissementen bedoeld in het eerste lid, eerste streepje, zijn vastgesteld in artikel 4 van de bijlage bij het Gerechtelijk Wetboek.

De grenzen van de politiezones bedoeld in het eerste lid, tweede streepje, zijn die welke zijn vermeld in de bijlage bij het koninklijk besluit van 24 oktober 2001 houdende de benaming van de politiezones.

De directie, bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt, stuurt de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone naar het Controleorgaan op de politionele informatie, dat binnen een maand na ontvangst van alle daartoe vereiste gegevens, deze valideert. Het Controleorgaan kan, met het oog op deze validatie, al de bevoegdheden uitoefenen die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018.

De statistieken en de bewaringstermijnen worden door de directie bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt aan de door de Koning aangewezen dienst toegezonden, enkel nadat deze op de hoogte is gebracht van hun validatie door het Controleorgaan.

Op voorstel van de door de Koning aangewezen dienst stellen de ministers van Justitie en van Binnenlandse Zaken jaarlijks de lijst vast van de gerechtelijke arrondissementen en de politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn.

Na deze vaststelling, zendt de door de Koning aangewezen dienst de lijst van de gerechtelijke arrondissementen en politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn, naar de operatoren.

§ 2. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse, waar het dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones.

Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse dit onmiddellijk mee aan de dienst aangewezen door de Koning, zodat deze dienst de nodige maatregelen kan nemen om de operatoren in te lichten en tot een algemene en ongedifferentieerde bewaring van de gegevens bedoeld in artikel 126/2, § 2, over te gaan voor het gehele grondgebied.

De bewaarplicht bedoeld in het tweede lid wordt bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. Bij ontstentenis van bevestiging bij koninklijk besluit, bekendgemaakt binnen de maand na de in het tweede lid bedoelde beslissing, wordt de gegevensbewaring opgeheven en worden de operatoren daarvan zo spoedig mogelijk in kennis gesteld door de dienst aangewezen door de Koning. Na deze kennisgeving vernietigen de operatoren de tot dan toe en voor dit doel bewaarde gegevens.

§ 3. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:

a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2, 3° tot 5°, van het Belgisch Scheepvaartwetboek;

b) de spoorwegstations in de zin van artikel 2, 5°, van de wet van 27 april 2018 op de politie van de spoorwegen;

c) de metro- en de pre-metrostations;

d) de luchthavens in de zin van artikel 2, punt 1), van Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van Verordening

(EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU, alsook de entiteiten die de bijbehorende installaties bedienen welke zich op de luchthavens bevinden;

e) de gebouwen bestemd voor de administratie van douane en accijnzen;

f) de gevangenissen in de zin van artikel 2, 15°, van de basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van de gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gepleegd, bedoeld in artikel 606 van het Wetboek van strafvordering, en de forensisch psychiatrische centra, bedoeld in artikel 3, 4°, c), van de wet van 5 mei 2014 betreffende de internering;

g) de wapenhandelaars en schietstanden zoals bedoeld in artikel 2, 1° en 19°, van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens;

h) de inrichtingen bedoeld in artikel 3.1.a), van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;

i) de inrichtingen bedoeld in artikel 2, 1°, van het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;

j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de uitvoeringsbesluiten ervan; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;

k) de zetel van de NV Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en gecodeerde communicatie- en informatiesysteem bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

l) de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op basis van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

m) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.

§ 4. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, dit wil zeggen:

a) voor de openbare orde, de neutrale zones bedoeld in artikel 3 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten, en de ministeriële beleidscellen;

b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de

Algemene Dienst Inlichting en Veiligheid wordt opgesteld op voorstel van de minister van Justitie en de minister van Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;

c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;

d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:

i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;

ii) de gemeentehuizen en de stadhuizen;

iii) het koninklijk paleis;

iv) de koninklijke domeinen;

v) de gebouwen toegewezen aan de instellingen bedoeld in titel III, hoofdstukken 5 tot 7 van de Grondwet;

vi) de gemeenten waar zich militaire domeinen bevinden;

vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;

e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;

f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid:

i) de ziekenhuizen bedoeld in artikel 2 van de gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;

ii) de Nationale Bank van België;

g) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.

§ 5. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, dit wil zeggen:

a) de ambassades en diplomatieke vertegenwoordigingen;

b) de gebouwen bestemd voor de Europese Unie;

c) de gebouwen en de infrastructuren bestemd voor de NAVO;

d) de instellingen van de Europese Economische Ruimte;

e) de instellingen van de Verenigde Naties;

f) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.

§ 6. Voor elke categorie van zone bedoeld in de paragrafen 3 tot 5, bepaalt de Koning de omvang van de perimeter van de zone.

Elke autoriteit die bevoegd is voor een van de aangelegenheden bedoeld in de paragrafen 3 tot 5, deelt jaarlijks op de door de Koning vastgestelde datum alleen aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de concrete vaststelling van de geografische zones.

Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten alleen deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld artikel 126/1, § 1, in deze zone zo spoedig mogelijk kan worden beëindigd.

Met uitzondering van de in paragraaf 4, b), bedoelde lijst van plaatsen, die door de inlichtingen-

en veiligheidsdiensten exclusief ter beschikking van het Vast Comité I wordt gesteld, stelt de door de Koning aangewezen dienst de bijgewerkte lijst van zones bedoeld in de paragrafen 3 tot 5 waar de gegevensbewaring verplicht is, ter beschikking van het Controleorgaan op de politionele informatie en van het Vast Comité I, elk binnen het kader van hun bevoegdheden.

Het Controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of het met redenen omklede bevel geven dat bepaalde geografische zones bedoeld in de paragrafen 3 tot 5, van de lijst geschrapt worden.

Op voorstel van de door de Koning aangewezen dienst stellen de minister van Defensie, de minister van Justitie, en de minister van Binnenlandse Zaken jaarlijks en bij elke wijziging bedoeld in het vijfde lid de lijst vast van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn.

Het ministeriële besluit bedoeld in het zesde lid wordt bekendgemaakt via vermelding in het Belgisch Staatsblad.

Na deze goedkeuring, zendt de door de Koning aangewezen dienst de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, naar de operatoren.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de gegevens die door de bevoegde autoriteiten aan de door de Koning aangewezen dienst worden meegedeeld of van de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, of zijn medewerking verleent aan de uitvoering van dit artikel, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

c. <u>Systematisering van de in de geografische zones te bewaren gegevens en van de bedoelde geografische zones</u>

56. Te bewaren gegevens

Artikel 126/2 § 2 bepaalt de gegevens die de operatoren moeten bewaren in het kader van de geografische zones.

Het zijn: de beschrijving en technische karakteristieken die werd aangewend tijdens de communicatie; bepaalde identificatiegegevens van de geadresseerde van de communicatie bedoeld in artikel 126 §1, 2°, 10° tot 14° en 16°; het IP-adres van de geadresseerde, het tijdstempel…; identificatie van alle lijnen bij groepsgesprek of doorschakeling; datum en exacte tijdstip aanvang en einde sessie; gegevens identificatie en locatie van aansluitpunten communicatie, van start tot einde, en exacte data en tijdstippen locaties; het geüploade en gedwonloade volume; datum en tijdstip verbinding van eindapparatuur met netwerk zowel opstart als uitschakeling; locatie eindapparatuur en datum en tijdstip locatie; andere identifiers met betrekking tot geadresseerde, tot zijn eindapparatuur.

Bij KB kunnen vermelde gegevens gepreciseerd worden.

57. Geografische zones

Artikel 126/3 bepaalt vijf geografische zones waarbij onder bepaalde voorwaarden de bewaring van gegevens door de operatoren kan bevolen worden.

§ 1. Gerechtelijke arrondissementen en politiezones met een bepaald aantal minimum aan misdrijven in de voorbije drie kalenderjaren.

§2. Geografische zones bepaald door het Coördinatieorgaan voor de Dreigingsanalyse met ten minste dreigingsniveau 3.

§3. Gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit.

§4. Zones waar er mogelijk ernstige bedreiging is voor de vitale belangen van land of de essentiële behoeften van de bevolking.

§5. Zones waar er mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen.

Onder §6 wordt dan bepaald dat de omvang van de perimeter van de zone voor elke categorie bepaald in paragrafen 3 tot 5, door KB wordt bepaald.

d. <u>Het standpunt van het Hof van Justitie EU</u>

58. Het arrest HvJ SpaceNet AG sprak zich uit over maatregelen die voorzien in een gerichte bewaring en in een spoedbewaring (punten 104-124).

Het huidig verzoek zal vanuit deze twee benaderingen toegepast worden op artikel 126/3.

Maatregelen die voorzien in een gerichte bewaring, een spoedbewaring (of een bewaring van IP-adressen)

104 Wat in de **derde plaats** de wettelijke maatregelen betreft die voorzien in **gerichte en spoedbewaring** van verkeers- en locatiegegevens, geven bepaalde door de lidstaten uiteengezette overwegingen ten aanzien van die maatregelen blijk van een striktere opvatting van de draagwijdte van deze maatregelen dan die welke wordt gehuldigd in de in punt 75 van het onderhavige arrest vermelde rechtspraak. Overeenkomstig wat in punt 57 van dit arrest in herinnering is gebracht, moeten die bewaringsmaatregelen weliswaar een uitzondering vormen op het bij richtlijn 2002/58 ingevoerde stelsel, maar deze richtlijn – gelezen in het licht van de in de artikelen 7, 8 en 11 alsook artikel 52, lid 1, van het Handvest erkende grondrechten – maakt de **mogelijkheid om een gerichte bewaring te gelasten niet afhankelijk van de voorwaarde dat vooraf bekend is op welke plaatsen een daad van zware criminaliteit kan worden gepleegd of welke personen ervan verdacht worden bij een dergelijke daad betrokken te zijn**. **Evenmin vereist die richtlijn dat het bevel tot spoedbewaring enkel ziet op verdachten die vóór dat**

bevel geïdentificeerd zijn (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 75).

105 Wat **ten eerste de gerichte bewaring** betreft, heeft het Hof geoordeeld dat artikel 15, lid 1, van richtlijn 2002/58 zich niet verzet tegen een op **objectieve factoren gebaseerde nationale wettelijke regeling** die ziet op personen van wie de verkeers- en locatiegegevens een – op zijn minst indirect – verband met daden van **zware criminaliteit** aan het licht kunnen brengen, een **bijdrage kunnen leveren tot de bestrijding van zware criminaliteit dan wel een ernstig risico voor de openbare veiligheid of een risico voor de nationale veiligheid kunnen voorkomen** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 76 en aldaar aangehaalde rechtspraak).

106 In zoverre heeft het Hof verduidelijkt dat die **objectieve factoren** weliswaar kunnen verschillen naargelang van de getroffen maatregelen voor het voorkomen, onderzoeken, opsporen en vervolgen van **zware criminaliteit**, maar dat de aldus beoogde **personen** met name degenen kunnen zijn die **voorafgaandelijk in het kader van de toepasselijke nationale procedures, op basis van objectieve en niet-discriminatoire factoren zijn geïdentificeerd als personen die een bedreiging vormen voor de openbare veiligheid of de nationale veiligheid van de betrokken lidstaat** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 77).

107 De lidstaten hebben dan ook onder meer de mogelijkheid om **bewaringsmaatregelen** te nemen ten aanzien van **personen** die op basis van een **dergelijke identificatie** het voorwerp zijn van een onderzoek of andere actuele surveillancemaatregelen dan wel personen die in het nationale strafregister zijn opgenomen met vermelding van een eerdere veroordeling wegens daden van zware criminaliteit en die mogelijkerwijs een hoog risico op recidive inhouden. Wanneer die identificatie berust op objectieve, niet-discriminatoire factoren die in het nationale recht worden omschreven, is de gerichte bewaring ten aanzien van de aldus geïdentificeerde personen gerechtvaardigd (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 78).

108 Daarnaast kan een **maatregel die voorziet in de gerichte bewaring** van verkeers- en locatiegegevens, naargelang van de keuze van de nationale wetgever en **met strikte inachtneming van het evenredigheidsbeginsel,** ook worden gebaseerd op een **geografisch criterium** wanneer de bevoegde nationale autoriteiten op basis van objectieve en niet-discriminatoire factoren van mening zijn dat zich in een of meer geografische zones een **situatie** voordoet die wordt gekenmerkt door een **hoog risico dat er daden van zware criminaliteit worden voorbereid of gepleegd. Deze zones kunnen onder meer plaatsen zijn waar een groot aantal daden van zware criminaliteit wordt gepleegd, plaatsen waar het risico op het plegen van dergelijke daden bijzonder hoog is, zoals plaatsen of infrastructuren die regelmatig door een zeer groot aantal personen worden bezocht, of strategische plaatsen, bijvoorbeeld luchthavens, stations, zeehavens of tolzones** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 79 en aldaar aangehaalde rechtspraak).

109 Benadrukt moet worden dat de bevoegde nationale autoriteiten volgens die rechtspraak voor de in het vorige punt bedoelde zones een gerichte bewaringsmaatregel kunnen treffen op basis van een geografisch criterium, zoals **het gemiddelde criminaliteitscijfer in een geografische zone, zonder dat zij noodzakelijkerwijs over concrete aanwijzingen hoeven te beschikken dat er in de betreffende zones daden van zware criminaliteit worden voorbereid of gepleegd**. Voor zover een gerichte bewaring op basis van een dergelijk criterium – naargelang van de ernstige strafbare feiten in kwestie en de specifieke situatie in de onderscheiden lidstaten – betrekking kan hebben op zowel plaatsen waar een groot aantal daden van zware criminaliteit wordt gepleegd als plaatsen waar het risico op het plegen van dergelijke daden bijzonder hoog is, kan die bewaring in beginsel ook niet leiden tot discriminatie, aangezien het criterium dat gebaseerd is op het gemiddelde zware-criminaliteitscijfer als zodanig geen verband houdt met mogelijkerwijs discriminerende factoren (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 80).

110 Een gerichte bewaringsmaatregel die betrekking heeft op **plaatsen of infrastructuren die regelmatig worden bezocht door een zeer groot aantal personen of op strategische plaatsen, zoals luchthavens, stations, zeehavens of tolzones, stelt de bevoegde autoriteiten bovendien en vooral in staat om verkeers- en met name locatiegegevens te verzamelen van al wie op een bepaald tijdstip op een van die plaatsen een elektronische-communicatiemiddel gebruikt.** Een dergelijke maatregel van gerichte bewaring kan die autoriteiten bijgevolg in staat stellen om via de toegang tot de aldus bewaarde gegevens informatie te verkrijgen over de aanwezigheid van die personen op de plaatsen of in de geografische zones waarop die maatregel betrekking heeft, alsmede over hun verplaatsingen daartussen of daarbinnen, en om uit deze informatie met het oog op de bestrijding van zware criminaliteit conclusies te trekken over de aanwezigheid en de activiteiten van die personen op die plaatsen of binnen die geografische zones op een bepaald tijdstip in de bewaringsperiode (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 81).

111 Tevens zij erop gewezen dat de **geografische zones** waarop een dergelijke gerichte bewaring betrekking heeft, **kunnen en in voorkomend geval moeten worden gewijzigd** indien de omstandigheden wijzigen die de selectie ervan rechtvaardigden, zodat met name kan worden ingespeeld op **evoluties in de strijd tegen zware criminaliteit**. Het Hof heeft namelijk reeds geoordeeld dat de in de punten 105 tot en met 110 van het onderhavige arrest beschreven maatregelen die voorzien in gerichte gegevensbewaring, **niet langer mogen gelden dan strikt noodzakelijk is in het licht van de met deze maatregelen nagestreefde doelstelling en van de omstandigheden waardoor die maatregelen worden gerechtvaardigd, hetgeen niet in de weg staat aan de eventuele verlenging ervan mocht de noodzaak van dergelijke bewaring blijven bestaan** (arresten van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 151, en 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 82).

112 Wat betreft de mogelijkheid om in andere onderscheidende criteria dan een persoonlijk of geografisch criterium te voorzien voor een gerichte bewaring van verkeers- en locatiegegevens, valt het niet uit te sluiten dat er andere objectieve en niet-discriminatoire criteria in aanmerking kunnen worden genomen om te waarborgen dat een gerichte bewaring niet verder gaat dan

wat strikt noodzakelijk is en om een – op zijn minst indirect – verband te leggen tussen daden van zware criminaliteit en de personen van wie de gegevens worden bewaard. Aangezien artikel 15, lid 1, van richtlijn 2002/58 betrekking heeft op wettelijke maatregelen van de lidstaten, staat het evenwel aan de lidstaten en niet aan het Hof om dergelijke criteria vast te stellen, **met dien verstande dat aldus niet opnieuw een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens mag worden ingevoerd** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 83).

113 Zoals de advocaat-generaal in punt 50 van zijn conclusie heeft opgemerkt, kunnen **eventuele moeilijkheden om tot een nauwkeurige omschrijving te komen van de gevallen waarin en de voorwaarden waaronder een gerichte bewaring toelaatbaar is, hoe dan ook niet rechtvaardigen dat de lidstaten een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens voorschrijven door van de uitzondering de regel te maken** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 84).

114 Wat **ten tweede de spoedbewaring** betreft van de verkeers- en locatiegegevens die door aanbieders van elektronische-communicatiediensten worden verwerkt en opgeslagen op grond van de artikelen 5, 6 en 9 van richtlijn 2002/58 dan wel op grond van krachtens artikel 15, lid 1, van deze richtlijn vastgestelde wettelijke maatregelen, zij eraan herinnerd dat die gegevens in beginsel **moeten worden gewist of geanonimiseerd** – naargelang van het geval – na het verstrijken van de wettelijke termijnen waarbinnen zij moeten worden verwerkt en opgeslagen volgens de nationale bepalingen tot omzetting van die richtlijn. Het Hof heeft niettemin geoordeeld dat zich bij de verwerking en opslag van die gegevens **situaties kunnen voordoen die ertoe nopen de betreffende gegevens ook na het verstrijken van die termijnen te bewaren** om ernstige strafbare feiten of aantastingen van de nationale veiligheid op te helderen, niet alleen wanneer die feiten of aantastingen reeds konden worden vastgesteld maar ook wanneer er na een objectief onderzoek van alle relevante omstandigheden een redelijk vermoeden bestaat dat dergelijke feiten zijn begaan of dat dergelijke aantastingen hebben plaatsgevonden (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 85).

115 In een dergelijke situatie staat het de lidstaten vrij om – gelet op de in de punten 65 tot en met 68 van het onderhavige arrest genoemde noodzaak om de rechten en legitieme belangen in kwestie met elkaar te verzoenen – bij een op grond van artikel 15, lid 1, van richtlijn 2002/58 vastgestelde wettelijke regeling te voorzien in de mogelijkheid om bij **een aan effectieve rechterlijke toetsing onderworpen besluit van de bevoegde autoriteit aan de aanbieders van elektronische-communicatiediensten het bevel te geven tot spoedbewaring, gedurende een bepaalde periode,** van de verkeers- en locatiegegevens waarover zij beschikken (arresten van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 163, en 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 86).

116 Aangezien de doelstelling van een dergelijke spoedbewaring niet meer beantwoordt aan de doelstellingen waarvoor de gegevens oorspronkelijk zijn verzameld en bewaard, en aangezien krachtens artikel 8, lid 2, van het Handvest elke verwerking van gegevens bepaalde doeleinden

moet dienen, moeten de lidstaten in hun wettelijke regeling **duidelijk maken voor welk doeleinde de spoedbewaring van gegevens mogelijk is.** Gelet op het feit dat een dergelijke bewaring een ernstige inmenging in de in de artikelen 7 en 8 van het Handvest erkende grondrechten kan vormen, kunnen enkel de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid die inmenging rechtvaardigen, mits deze maatregel en de toegang tot de aldus bewaarde gegevens niet verder gaat dan wat strikt noodzakelijk is, zoals is uiteengezet in de punten 164 tot en met 167 van het arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791) (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 87).

117 Het Hof heeft gepreciseerd dat **dit soort bewaringsmaatregel niet** hoeft te worden **beperkt tot de gegevens van personen die voorafgaandelijk zijn geïdentificeerd als personen die een bedreiging vormen voor de openbare veiligheid of de nationale veiligheid van de betrokken lidstaat, dan wel tot de gegevens van personen op wie een concrete verdenking rust dat zij een daad van zware criminaliteit hebben gepleegd of de nationale veiligheid hebben ondermijnd.** Volgens het Hof kan een dergelijke maatregel – mits daarbij het kader in acht wordt genomen dat is ingesteld bij artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 alsook artikel 52, lid 1, van het Handvest, en gelet op de overwegingen in punt 70 van het onderhavige arrest – namelijk naar keuze van de nationale wetgever en binnen de grenzen van het strikt noodzakelijke worden uitgebreid tot verkeers- en locatiegegevens die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig strafbaar feit te hebben gepleegd of de nationale veiligheid te hebben aangetast dan wel plannen daarvoor hebben gemaakt, voor zover die gegevens op basis van objectieve en niet-discriminatoire factoren kunnen bijdragen tot de opheldering van een dergelijk strafbaar feit of een dergelijke aantasting van de nationale veiligheid, zoals de gegevens van het slachtoffer van het strafbare feit of de aantasting en de gegevens van personen uit de sociale of professionele omgeving van het slachtoffer (arresten van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 165, en 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 88).

118 Derhalve kan een wettelijke maatregel toestaan dat aan aanbieders van elektronische-communicatiediensten het bevel wordt gegeven tot **spoedbewaring** van de verkeers- en locatiegegevens van onder meer **personen met wie een slachtoffer** via zijn elektronische-communicatiemiddelen **contact had** voordat er zich een ernstige bedreiging voor de openbare veiligheid voordeed of er een daad van zware criminaliteit werd gepleegd (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 89).

119 Volgens de in punt 117 van het onderhavige arrest in herinnering gebrachte rechtspraak van het Hof en onder dezelfde voorwaarden als die welke in dat punt zijn genoemd, kan een dergelijke **spoedbewaring ook worden uitgebreid tot bepaalde geografische zones**, zoals de **plaats waar het betreffende strafbare feit of de betreffende aantasting van de nationale veiligheid heeft plaatsgevonden of is voorbereid.** Gepreciseerd dient te worden dat een dergelijke maatregel tevens kan worden getroffen ten aanzien van verkeers- en locatiegegevens die betrekking hebben op de plaats waar een persoon, die mogelijkerwijs het slachtoffer is geworden van een daad van zware criminaliteit, is verdwenen, op voorwaarde dat die maatregel en de toegang tot

de aldus bewaarde gegevens niet verder gaan dan wat strikt noodzakelijk is voor de bestrijding van zware criminaliteit of voor de bescherming van de nationale veiligheid, zoals is uiteengezet in de punten 164 tot en met 167 van het arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791) (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 90).

120 Bovendien moet worden verduidelijkt dat artikel 15, lid 1, van richtlijn 2002/58 er niet aan in de weg staat dat de bevoegde nationale autoriteiten **een spoedbewaringsmaatregel gelasten vanaf de eerste fase van het onderzoek naar een ernstige bedreiging voor de openbare veiligheid of een eventuele daad van zware criminaliteit,** dat wil zeggen vanaf het tijdstip waarop die autoriteiten volgens de relevante nationaalrechtelijke bepalingen een dergelijk onderzoek kunnen openen (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 91).

121 Wat de verschillende **in punt 75 van het onderhavige arrest genoemde bewaringsmaatregelen** voor verkeers- en locatiegegevens betreft, zij er nog op gewezen dat deze naar keuze van de nationale wetgever en **binnen de grenzen van het strikt noodzakelijke tegelijkertijd kunnen worden toegepast.** Artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 alsook artikel 52, lid 1, van het Handvest, zoals uitgelegd in de rechtspraak die voortvloeit uit het arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791), verzet zich bijgevolg niet tegen een combinatie van die maatregelen (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 92).

122 In de **vierde en laatste plaats** moet worden benadrukt dat de **evenredigheid** van de op grond van artikel 15, lid 1, van richtlijn 2002/58 getroffen maatregelen volgens de vaste rechtspraak van het Hof zoals die is samengevat in het arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791), **niet alleen vereist dat die maatregelen passend en noodzakelijk zijn, maar ook dat zij evenredig zijn aan de nagestreefde doelstelling** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 93).

123 In dit verband zij eraan **herinnerd** dat het Hof in punt 51 van zijn arrest van 8 april 2014, Digital Rights Ireland e.a. (C-293/12 en C-594/12, EU:C:2014:238), heeft geoordeeld dat ofschoon de **bestrijding van zware criminaliteit** van eminent belang is voor het waarborgen van de openbare veiligheid en de doeltreffendheid ervan in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken, een dergelijke doelstelling van algemeen belang – hoe essentieel zij ook is – **op zichzelf beschouwd niet kan rechtvaardigen dat een maatregel die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens,** zoals die welke is ingevoerd bij richtlijn 2006/24, noodzakelijk wordt geacht (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 94).

124 **In dezelfde gedachtegang** heeft het Hof in punt 145 van het arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791), verduidelijkt dat zelfs de positieve verplichtingen die voor de lidstaten, naargelang van het geval, kunnen voortvloeien

uit de artikelen 3, 4 en 7 van het Handvest en die – zoals in punt 64 van het onderhavige arrest is opgemerkt – betrekking hebben op de invoering van regels die de **effectieve bestrijding van strafbare feiten** mogelijk maken, **geen dermate ernstige inmengingen** in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten kunnen rechtvaardigen als die welke besloten liggen in een nationale wettelijke **regeling die voorziet in een bewaring van verkeers- en locatiegegevens van vrijwel de gehele bevolking, zonder dat de gegevens van de betrokken personen een – op zijn minst indirect – verband met de nagestreefde doelstelling aan het licht kunnen brengen** (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 95).

e. Systematisering arrest Hof van Justitie EU

59. *Gerichte bewaring* is mogelijk op basis van een nationale regeling gebaseerd op objectieve factoren voor bestrijding zware criminaliteit, voor het voorkomen van een ernstig risico voor de openbare veiligheid of de nationale veiligheid.

    Gerichte bewaring kan gebaseerd worden op een geografisch criterium met strikte inachtneming van het evenredigheidsbeginsel, op basis van objectieve en niet-discriminatoire factoren dat er een hoog risico bestaat dat er daden van zware criminaliteit worden voorbereid of gepleegd. Deze zones kunnen onder meer plaatsen zijn waar een groot aantal daden van zware criminaliteit wordt gepleegd, plaatsen waar het risico op het plegen van dergelijke daden bijzonder hoog is, zoals plaatsen of infrastructuren die regelmatig door een zeer groot aantal personen worden bezocht, of strategische plaatsen, bijvoorbeeld luchthavens, stations, zeehavens of tolzones.

    Geografisch criterium kan zijn het gemiddelde criminaliteitscijfer in een geografische zone, zonder dat er noodzakelijk concrete aanwijzingen hoeven te zijn dat in die zone zware criminaliteit wordt voorbereid of gepleegd.

    Geografische zones kunnen en in voorkomend geval moeten worden gewijzigd om in te spelen op evoluties in strijd tegen zware criminaliteit.

60. *Spoedbewaring* is mogelijk om ernstige strafbare feiten of aantastingen van de nationale veiligheid op te helderen. Vereist is een besluit van de bevoegde autoriteit dat aan een effectieve rechterlijke toetsing onderworpen is. De doelstelling van de spoedbewaring moet duidelijk in de wettelijke regeling opgenomen zijn. Spoedbewaring kan uitgebreid worden tot bepaalde geografische zones.

61. *Gerichte bewaring en spoedbewaring* moeten voldoen aan volgende *voorwaarden*.

    Criteria geografische zones mogen niet verder gaan dan het strikt noodzakelijke en ‘met dien verstande dat aldus niet opnieuw een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens mag worden ingevoerd.’

Maatregelen gerichte bewaring mogen niet langer gelden dan strikt noodzakelijk is in het licht van de met deze maatregelen nagestreefde doelstelling en van de omstandigheden waardoor die maatregelen worden gerechtvaardigd, maar met mogelijkheid op verlenging als noodzaak bewaring blijft bestaan.

Benadrukt dat de maatregelen passend en noodzakelijk zijn en evenredig met het nagestreefde doel.

Herinnert er aan dat bestrijding zware criminaliteit op zichzelf beschouwd niet kan rechtvaardigen dat een maatregel die voorziet in algemene en ongedifferentieerde bewaring noodzakelijk wordt geacht.

Moeilijkheden om tot een nauwkeurige omschrijving van de gevallen van gerichte bewaring te komen, kan hoe dan ook niet rechtvaardigen dat de lidstaten een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens voorschrijven door van de uitzondering de regel te maken. In dezelfde gedachtegang: effectieve bestrijding strafbare feiten rechtvaardigen geen dermate ernstige inmengingen in de grondrechten die voor gevolg heeft dat de gegevens van vrijwel de gehele bevolking in bewaring worden genomen zonder dat er – op zijn minst indirect – verband is met de nagestreefde doelstelling.

f. <u>Discussie en toepassing</u>

62. Het betreft de verplichte bewaring door de operatoren van bepaalde gegevens in vijf welbepaalde gebieden of zones. Vermelde bepalingen moeten beoordeeld worden in hun geheel en ieder op zich. Het is mogelijk dat de verplichte bewaring beperkt wordt tot één of meerdere zones; het is eveneens mogelijk dat op basis van deze wetsbepalingen de verplichte bewaring betrekking heeft op alle zones.

63. De in die zones te bewaren gegevens op basis van artikel 126/2 § 2 zijn op zich dermate dat zij niet beantwoorden aan de in het middel vermelde wettelijke bepalingen. Verzoeker herneemt hier op dit punt het tweede onderdeel van het middel. Ook wat de vermelde zones betreft voorziet de maatregel in een algemene en ongedifferentieerde bewaring van het merendeel van de verkeers- en locatiegegevens, voor een periode van zes tot twaalf maanden (126/3 §1), voor een in de wet niet bepaalde periode (126/3 §2) en voor een bij KB te bepalen periode (126/3 §§ 3-5).

Specifiek komt de tekst van artikel 126/2 §2 er op neer dat locatiegegevens bewaard worden van personen die zich niet in de geografische zone bevinden waarvoor moet bewaard worden. Zo bepaalt artikel 126/2 § 2, 6° dat gegevens moeten bewaard worden die de identificatie en lokalisatie van de cellen of andere netwerkaansluitpunten van het mobiele netwerk mogelijk maken, die werden gebruikt voor de communicatie, van de start tot het einde van de communicatie, alsook de exacte data en tijdstippen van deze verschillende locaties. Bijgevolg zijn ook gegevens geviseerd van communicatie die start buiten de zone en eindigt in de zone, én van communicatie die start binnen de zone, maar eindigt buiten de zone. Komt daar nog bij dat ook aan de operatoren van 'onderliggende elektronische communicatienetwerken' die bewaarplicht wordt opgelegd. Ook in die zin laat vermeld artikel een zeer ruime dataretentie mogelijk.

64. De discussie betreft inzonderheid de overeenstemming van de bewaring in de vijf vermelde zones ieder op zich, en de bewaring in een deel of het geheel van de vermelde zones. De discussie betreft

ook het gebrek aan realiteitszin en toepasbaarheid van de wetgeving. Verder betreft de discussie de bewaringstermijnen die betrekking hebben op de verschillende situaties van artikel 126/3 en specifiek wat artikel 126/3 §§3-5 betreft de omvang van de perimeter van de zones.

E.1. Wat betreft de bewaringstermijnen van artikel 126/3

65. Artikel 126/3 is op zich problematisch wat betreft de vooropgestelde periodes van bewaring. In tegenstelling tot de vernietigde Duitse TKG-wet waar het ging over periodes van vier tot tien weken, voorziet de betreden wet in ofwel veel langere periodes, ofwel niet bepaalde periodes.

    Het gaat om een algemene en ongedifferentieerde bewaring van het merendeel van de verkeers- en locatiegegevens, voor een periode van zes tot twaalf maanden (126/3 §1), voor een in de wet niet bepaalde periode (126/3 §2) en voor een bij KB te bepalen periode (126/3 §§ 3-5). Zij beantwoorden niet aan de vereiste van 'een periode die niet langer is dan strikt noodzakelijk'. (SpaceNet, 75)

    De bewaringstermijn van zes tot twaalf maanden met betrekking tot artikel 126/3 §1 (zones criminaliteit) zijn wat de duur betreft van die omvang dat zij toelaten precieze informatie over het privéleven van de gebruiker van het elektronische-communicatiemiddel te verschaffen. Het HvJ oordeelde in die zin negatief over de veel kortere bewaringstermijnen (vier tot tien weken) in de Duitse TKG-wet. (SpaceNet AG, punt 89).

66. Voor wat betreft 126/3 §2 (zone bepaald door optreden OCAD) geldt de verplichting tot algemene bewaring op het hele grondgebied zo het OCAD dreigingsniveau 3 vaststelt voor het ganse grondgebied. Het OCAD deelt dit mee 'aan de dienst aangewezen door KB' die de operatoren 'inlicht' 'over te gaan tot een ongedifferentieerde bewaring op het ganse grondgebied'. De bewaarplicht moet dan bevestigd worden bij KB; wanneer deze bevestiging er niet komt wordt de gegevensbewaring opgeheven. De periode is bijgevolg niet duidelijk. Er is niet voorzien hoe en door wie die bewaring zal opgeheven worden; er is niet bepaald dat die bewaringsplicht stopt als niveau 3 wordt opgeheven. Er is enkel voor een bewaring op het ganse grondgebied een negatieve bepaling dat die bewaringsplicht stopt in geval het KB er niet binnen de maand na het inlichten van de operatoren komt.

67. De in de wet niet bepaalde bewaringstermijn met betrekking tot de zones opgenomen in artikel 126/3 §§3-5 (drie zones) is eveneens niet in overeenstemming met het verbod op een algemene en ongedifferentieerde bewaring. De wet die voorziet dat de bewaartermijn bij KB bepaald wordt, bepaalt niet eens welke minimum- en maximumtermijnen door het KB moeten gerespecteerd worden. Door deze bewaringstermijn te laten bepalen door een KB en niet vast te leggen in de wet zelf, beantwoordt die bepaling niet aan de vereiste dat de maatregelen door middel van duidelijke en nauwkeurige regels moeten waarborgen dat de gegevens slechts bewaard worden als aan de geldende materiële en procedurele voorwaarden is voldaan. (SpaceNet, punt 75; Quadrature du Net, punt 168).

E.2 Wat betreft het artikel 126/3 §1 geografische zones criminaliteit

68. Wettelijke bepaling

De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones bestaande uit:

- de gerechtelijke arrondissementen waar minstens drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren;
- de politiezones waar minstens drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, en die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan drie strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, eerste streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2: …

De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld over een gemiddelde van de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet van 5 augustus 1992 op het politieambt. …

Op voorstel van de door de Koning aangewezen dienst stellen de ministers van Justitie en van Binnenlandse Zaken jaarlijks de lijst vast van de gerechtelijke arrondissementen en de politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn.

Na deze vaststelling, zendt de door de Koning aangewezen dienst de lijst van de gerechtelijke arrondissementen en politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn, naar de operatoren.

69. Standpunt Hof van Justitie EU

Het HvJ laat gerichte bewaring toe op basis van geografische zone in het kader van als deze gebaseerd is op objectieve factoren en als deze een bijdrage kunnen leveren tot de bestrijding van zware criminaliteit (SpaceNet, 105). De voorwaarden hierbij zijn: strikte in achtneming van het evenredigheidsbeginsel (SpaceNet, 108); zones gekenmerkt door hoog risico op daden zware criminaliteit (SpaceNet, 108); plaatsen bezocht door grote aantallen personen of strategische plaatsen (SpaceNet, 110); niet langer dan strikt noodzakelijk (SpaceNet, 111); moeilijkheden nauwkeurige omschrijving geen rechtvaardiging algemene en ongedifferentieerde bewaring (SpaceNet, 113), in achtname kader artikel 15, lid 1, Richtlijn 2002/58, gelezen in het licht van artikelen 7, 8 en 11 Handvest; gegevens die op objectieve en niet-discriminatoire factoren bijdragen tot het doel van de maatregel (SpaceNet, 117); binnen grenzen strikt noodzakelijke (SpaceNet, 121); passend, noodzakelijk, evenredig (SpaceNet, 122); geen dermate ernstige inmenging dat regeling voorziet in verkeers- en locatiegegevens van vrijwel hele bevolking (SpaceNet, 124).

70. Subonderdelen van het middel wat betreft artikel 126/3 §1

Eerste subonderdeel: de noodzaak in een democratische samenleving van bewaring van de gegevens in het kader van de zware criminaliteit is niet aangetoond.

71. Een essentiële voorwaarde is dat de maatregel ter bestrijding van de zware criminaliteit noodzakelijk moet zijn in een democratische maatschappij. Deze voorwaarde stelt de vereiste om te oordelen wat in een democratische maatschappij in dat kader noodzakelijk is. Essentieel is de invulling van het begrip 'democratische maatschappij'.

    De noodzaak is niet aangetoond. In de parlementaire debatten is gebleken dat de regering over geen enkel precies gegeven beschikt over de impact van dataretentie op de opheldering van zware criminaliteit. Nochtans is dit wetenschappelijk en statistisch na te gaan daar in België in de periode 2013 (eerste dataretentiewet) tot op datum van 20 juli 2022 (derde dataretentiewet) het land periodes heeft gekend van toepassing en niet-toepassing van deze wetgeving in het kader van opsporing en vervolging van zware criminaliteit.

72. 'De wetgeving over het bijhouden van communicatiegegevens zorgt al jaren voor juridische strijd. Antwerps procureur-generaal Patrick Vandenbruwaene opperde in zijn mercuriale dat het openbaar ministerie de impact van die gegevens op het onderzoek zou moeten opvolgen. Is de meegedeelde informatie nuttig gebleken? Heeft men zo een verdachte kunnen identificeren of een slachtoffer kunnen vinden? Die gegevens kunnen van belang zijn wanneer de dataretentie opnieuw verdedigd moet worden tegenover het recht op privacy en de bescherming van persoonsgegevens. Politiediensten, onderzoeksrechters en het College van procureurs-generaal zijn het er unaniem over eens dat het bevragen van metagegevens - verkeers- en locatiegegevens – absoluut noodzakelijk is om de waarheid in een onderzoek aan het licht te brengen. Privacy-experten zijn dan weer van mening dat misdrijven evengoed zonder deze gegevens kunnen worden opgelost. De wet op de bewaarplicht van communicatiegegevens werd al twee keer vernietigd door het Grondwettelijk Hof, in navolging van arresten van het Europees Hof van Justitie. Zowel op het federale als Europese niveau werd een debat gevoerd op basis van principes en assumpties, maar al te vaak zonder dat dit gestaafd werd door betrouwbare cijfers. Niet omdat de cijfers niet mededeelbaar waren, maar simpelweg omdat ze niet systematisch werden bijgehouden. Transparantie over cijfers kan een belangrijke bijdrage leveren aan het debat in de toekomst.' (Juristenkrant, 14 september 2022, p.8)

    Er zijn in België geen (statistische) data die de noodzaak van de maatregel rechtvaardigen.

73. In het rapport *'General data retention/effects on crime'* van 27 januari 2020 van de European Research Service van het Europees Parlement, werd in 18 EU-landen (België niet, omdat er geen statische gegevens waren) de impact van het al of niet bestaan van een dataretentiewet op de graad van opheldering van de criminaliteit onderzocht in de periode 2011-2018. Het rapport besluit: 'Blankety, indiscriminate telecommunications data retention has no statistically significant impact on crime or crime clearance'.

74. Met betrekking tot het gegeven dat dataretentie (g)een absolute noodzaak is voor de strafvervolging nam het HvJ volgende overweging:

'Dienaangaande zij in de eerste plaats opgemerkt dat de doeltreffendheid van strafvervolging doorgaans niet afhangt van één onderzoeksmiddel, maar van alle onderzoeksmiddelen waarover de bevoegde nationale autoriteiten te dien einde beschikken. (Commissioner of An Garda Siochana, punt 69; SpaceNet AG, punt 96).

De notie noodzakelijkheid vereist het bestaan van een dwingend sociaal imperatief en in het bijzonder dat de inmenging proportioneel is in verhouding tot het nagestreefde maatschappelijk doel. (EHRM, 25 maart 1992, Campbell c. Verenigd Koninkrijk, § 44).

75. Een essentiële voorwaarde om in het kader van de strijd tegen zware criminaliteit een maatregel van inmenging in de grondrechten van privacy en vrije elektronische communicatie te rechtvaardigen – met name de noodzakelijkheid van dergelijke inmenging – is niet aangetoond.

    Het is niet omdat het HvJ onder bepaalde voorwaarden in het kader van de strijd tegen zware criminaliteit inmenging toelaat, dat de concrete noodzaak hiervan in België ook is aangetoond.

    Tweede subonderdeel: de maatregel van artikel 126/3 §1 schendt de in het middel vermelde wettelijke bepalingen. De maatregel is niet in overeenstemming met de vereisten 'in een democratische maatschappij noodzakelijk, redelijk en proportioneel' en 'strikte evenredigheid met het nagestreefde doel'.

76. De maatregel van 126/3 §1 is niet gekoppeld aan strategische plaatsen of plaatsen bezocht door een groot aantal personen, maar enkel aan criminaliteitscijfers.

    Deze maatregel schept een permanente situatie, minstens een situatie van minimum één jaar, in die zin dat 'jaarlijks' een lijst met zones wordt aangewezen. Dit is weliswaar afhankelijk van het criminaliteitscijfer in de zone, maar gezien de relatief lage graad van strafbare feiten (drie tot zeven per duizend inwoners; 0,3% tot 0,7%) en de aard van de misdrijven gaat het om een te ruim criterium. De maatregel treft op zich ook de grote meerderheid van burgers (de 997 tot 993 anderen per duizend) die niets met strafbare feiten te maken hebben. Het is betwist dat de relatief lage graad van strafbare feiten het hoog risico kenmerkt, zelfs gezien de aard van de weerhouden strafbare feiten. De maatregel is niet evenredig en schendt de grondrechten van een grote meerderheid van burgers. (SpaceNet, punt 59). De maatregel van bewaring in arrondissementen en politiezones is opzichtig onwettig.

77. Zulks blijkt des te meer uit de volgende stellingen van vice-eersteminister Van Quickenborne, in het kader van diens inleidende uiteenzetting betreffende het ontwerp dat de bestreden wet: "*Indien na een zorgvuldige telling in elk gerechtelijk arrondissement en elke politiezone blijkt dat de zware criminaliteit op elk van deze plaatsen voldoende hoog is, zullen de gegevens gericht worden bewaard, maar zullen de gevolgen ervan algemeen zijn.*" en "*Het is dus mogelijk heel het grondgebied te dekken*.". Het vooropgestelde criterium is aldus, zoals reeds gesteld, te ruim, gelet op de (mogelijks) algemene gevolgen (Parl. St., Kamer, Doc 55 2572/003, p. 14).

    Dat de regering niet exact kan aangeven welk percentage van het grondgebied of van de bevolking onder het toepassingsgebied van de bestreden wet zal vallen, zoals opgemerkt door de heer Boukili

(Parl. St., Kamer, Doc 55 2572/003, p. 63), toont des te meer aan dat er geen sprake is van de vereiste evenredigheid.

78. De Gegevensbeschermingsautoriteit stelt dan ook: "*De wetgever moet de door hem weerhouden drempel rechtvaardigen en aantonen dat deze de facto niet kan leiden tot een verplichting tot algemene en ongedifferentieerde bewaring van de gegevens op (bijna) het hele nationale grondgebied. De wetgever moet er (…) op toezien dat de impact van deze drempel in de praktijk evenredig is met de huidige statistieken; dat zou niet het geval zijn als bij de inwerkingtreding van het voorontwerp van wet het hele nationale grondgebied (of toch bijna) "onder toezicht" zou worden geplaatst. De wetgever moet een strenge en kwantitatieve analyse maken van de evenredigheid van het criterium/de drempel.*" (Parl. St., Kamer, Doc 55 2572/001, p. 774-775).

79. Het criterium om strafbare feiten te weerhouden is artikel 90ter, §§ 2 tot 4 van het Wetboek van Strafvordering. Het betreft strafbare feiten waarvoor de onderzoeksrechter op basis van artikel 90ter § 1 een maatregel kan nemen van onderscheppen, kennisname, doorzoeken, opneming, zoeking in een informaticasysteem. Paragraaf 2 betreft een lijst van 45 misdrijven. Paragraaf 3 betreft een poging tot het plegen van een misdaad bedoeld in paragraaf 2. Paragraaf 4 handelt over een strafbaar feit bedoeld in de artikelen 322 of 323 Strafwetboek (vereniging van misdadigers). Het gaat om een te ruim criterium voor het bepalen van strafbare feiten in het kader van de dataretentie. Er moet opgemerkt worden dat de bevoegdheid van de onderzoeksrechter in het kader van artikel 90ter niet zonder meer als verantwoording kan dienen om dit artikel ook in het kader van de gegevensbewaring te hanteren. De onderzoeksrechter kan de maatregel alleen toepassen als voldaan is aan de voorwaarden van paragraaf 1 van vermeld artikel: uitzonderlijke gevallen, ernstige aanwijzingen voor het bestaan van het strafbaar feit, als overige middelen onderzoek niet volstaan, om de waarheid aan de dag te brengen, op grond van precieze aanwijzingen dat iemand verdacht wordt het feit te hebben gepleegd. Deze voorwaarden zijn niet aanwezig met betrekking tot het bewaren van die gegevens. Het gaat om een veralgemeende bewaring.

    Het gaat om het uitzonderlijk en subsidiair karakter van deze methode van inmenging in de grondrechten van artikel 7 en 8 Handvest en artikel 22 Grondwet in het kader van de strijd tegen zware criminaliteit. Deze mogelijkheid is voorbehouden aan de onderzoeksrechter en aan geen enkele andere autoriteit.

80. Het is betwistbaar dat de 45 strafbare feiten vermeld in artikel 90ter §§2 tot 4 van het Wetboek van Strafvordering (allen) beantwoorden aan het begrip zware criminaliteit. Zo zijn er onder deze feiten bijvoorbeeld misdrijven die bestraft worden met 3 maanden tot twee jaar (artikel 238), enz… Het begrip 'zware criminaliteit' in het kader waarvan gegevensbewaring eventueel mogelijk is, vereist een specifieke lijst van misdrijven. Artikel 90ter , §§2 tot 4 Wetboek Strafvordering is gemaakt met het oog op de specifieke bevoegdheid van de onderzoeksrechter, maar niet met het oog op het definiëren van het begrip 'zware criminaliteit' in het kader van de gegevensbewaring. De maatregel beantwoordt niet aan de voorwaarde 'wettelijke maatregel met het oog op bestrijding zware criminaliteit'. (SpaceNet, punt 75)

81. Ook het begrip 'strafbaar feit' is betwistbaar. Dit begrip kent op zich geen exacte wettelijke definitie in het strafwetboek. Het begrip maakt geen onderscheid tussen vervolging, veroordeling of niet-vervolging of seponering.

82. Verder is het betwistbaar dat op basis van statistische gegevens van de Algemene Nationale Gegevensbank (ANG) op een wetenschappelijke en objectieve wijze vermelde vaststellingen van het aantal strafbare feiten kan gebeuren. De ANG is niet met dit doel ontworpen. In de ANG wordt zowat alles opgeslagen wat kan verbonden worden aan strafbare feiten. De ANG bevat ook gegevens van slachtoffers. Op basis van de ANG is het niet mogelijk aan te tonen of het gaat om gewone (terechte of onterechte) meldingen van strafbare feiten, dan wel om feiten die effectief geleid hebben tot een schuldigverklaring. De ANG omvat in deze dus niet enkel feiten die werden gepleegd, voor de rechter gebracht en tot een veroordeling hebben geleid, terwijl het nochtans het aantal effectief gepleegde, strafbare feiten is dat de basis vormt om te bepalen of er aan bewaring gedaan kan worden in een bepaald arrondissement.

    Dat de ANG niet geschikt is voor het doeleinde dat voorgesteld is in de bestreden wet, is ook een mening die de Gegevensbeschermingsautoriteit is toegedaan. Die autoriteit "*stelt zich (immers) vragen bij de relevantie van het gebruik van de A.N.G. aangezien die in de databank wordt bijgehouden door de politie die van nature, gezien haar wettelijke opdracht, zal geneigd zijn om er alle vermoedens van strafbare feiten 90ter in op te nemen en/of, zoals het C.O.C. heeft benadrukt in zijn advies van 21 mei 2020, om een vermoeden van strafbaar feit al te makkelijk aan te merken als een vermoeden van ernstig misdrijf in de zin van artikel 90ter van het W.S.V. In die context meent de Autoriteit dat het passender zou zijn om een databank te gebruiken waarvan de kwaliteit van de statistische gegevens is vastgelegd bij wet, zoals de wet van 4 juli 1962 betreffende de openbare statistiek*." (Parl. St., Kamer, Doc 55 2572/001, p. 775).

    Bovendien heeft het COC in zijn jaarverslag van 2020 aangestipt dat "*de ANG heel wat onnauwkeurigheden en/of fouten bevat*", zoals "*de onjuiste kwalificatie van de feiten*", hetgeen opgemerkt werd door de heer Nabil Boukili (Parl. St., Kamer, Doc 55 2572/003, p. 35)

    De ANG als statistische referentie kan bijgevolg niet aangewend worden, op zich, en alleszins niet als rechtvaardiging voor de inmenging in de rechten van een massaal aantal personen.

83. Ten slotte, dat de procedure waarbij feiten worden geteld, nog aan het Controleorgaan op de politionele informatie ter controle moet worden voorgelegd (Parl. St., Kamer, Doc 55 2572/003, p. 20), maakt dat er op heden in ieder geval geen sprake kan zijn van een passende, noodzakelijke en evenredige maatregel.

E.3. Wat betreft het artikel 126/3 §2. Bewaring gegevens dreigingsniveau 3

84. Wettelijke bepaling

> § 2. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse, waar het dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2°, van de

wet van 10 juli 2006 betreffende de analyse van de dreiging, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones.

Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse dit onmiddellijk mee aan de dienst aangewezen door de Koning, zodat deze dienst de nodige maatregelen kan nemen om de operatoren in te lichten en tot een algemene en ongedifferentieerde bewaring van de gegevens bedoeld in artikel 126/2, § 2, over te gaan voor het gehele grondgebied.

De bewaarplicht bedoeld in het tweede lid wordt bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. Bij ontstentenis van bevestiging bij koninklijk besluit, bekendgemaakt binnen de maand na de in het tweede lid bedoelde beslissing, wordt de gegevensbewaring opgeheven en worden de operatoren daarvan zo spoedig mogelijk in kennis gesteld door de dienst aangewezen door de Koning. Na deze kennisgeving vernietigen de operatoren de tot dan toe en voor dit doel bewaarde gegevens.

Dit artikel betreft het bewaren van gegevens in het kader van de nationale en openbare veiligheid, waartoe OCAD bevoegd is.

85. Standpunt Hof van Justitie EU

86. Het HvJ laat spoedbewaring en op een geografische zone of het hele grondgebied gerichte bewaring toe in het kader van de bescherming van de nationale veiligheid, de bedreiging van de openbare veiligheid en de zware criminaliteit. (SpaceNet, 114-121). De voorwaarden hierbij zijn: wissen of anonimiseren tenzij objectieve noodzaak verdere bewaring (SpaceNet, 114); effectieve rechterlijke controle van besluit van de bevoegde autoriteit tot bewaring (SpaceNet, 115); duidelijk doeleinde spoedbewaring (SpaceNet, 116); in achtname kader artikel 15, lid 1, Richtlijn 2002/58, gelezen in het licht van artikelen 7, 8 en 11 Handvest; gegevens die op objectieve en niet-discriminatoire factoren bijdragen doel maatregel (SpaceNet, 117); binnen grenzen strikt noodzakelijke (SpaceNet, 121); passend, noodzakelijk, evenredig (SpaceNet, 122); geen dermate ernstige inmenging dat regeling voorziet in verkeers- en locatiegegevens van vrijwel hele bevolking (SpaceNet, 124).

In de arresten HvJ SpaceNet (punt 132) en La Quadrature du Net (punt 229), en in het arrest nr. 57/2021 van 22 april 2021 van het Belgisch Grondwettelijk met betrekking tot de tweede Belgische dataretentiewet en dat zich aansloot bij het arrest La Quadrature du Net, is gesteld dat algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens mogelijk is ter bescherming van de nationale veiligheid 'in situaties waarin de betrokken staat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit, waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer dan strikt noodzakelijk is, maar die kan worden verlengd indien die bedreiging voortduurt.'

87. Toepassing en discussie artikel 126/3 §2

88. Artikel 126/3 §2 bepaalt een onderscheid in bewaring naargelang in een bepaalde of bepaalde geografische zones het dreigingsniveau 3 is vastgesteld, dan wanneer dit dreigingsniveau het ganse grondgebied betreft.

    In het eerste geval is het blijkbaar het OCAD dat de plicht tot bewaren bepaalt en oplegt aan de operatoren (hoewel het artikel op dit punt niet duidelijk is). In het artikel is niet vermeld hoe deze bewaarplicht beëindigd wordt.

    In het tweede geval deelt het OCAD dit mee aan een dienst aangewezen bij KB, die de nodige maatregelen neemt om de operatoren in te lichten. In dit tweede geval moet de bewaarplicht binnen de maand bij KB bevestigd worden. Zo dit niet bevestigd wordt vervalt de bewaarplicht. Maar het artikel voorziet buiten dit automatisme in geval er binnen de maand geen KB is genomen, niet in de wijze waarop (wanneer er wel een KB is genomen) de bewaarplicht beëindigd wordt.

89. Te buiten gelaten de grote onduidelijkheden en lacunes in vermeld artikel, wordt gesteld dat de regeling op diverse punten niet in overeenstemming is met het standpunt van het HvJ in de arresten SpaceNet en La Quadrature du Net. Er is geen effectieve rechterlijke controle voorzien op het besluit van de bevoegde autoriteit. Ook stelt zich de vraag of het criterium van niveau 3 van de dreiging valt binnen de grenzen van passend, noodzakelijk, evenredig en beantwoordt aan het begrip 'werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid'. Niveau 3 of ernstig, is wanneer de dreiging mogelijk en waarschijnlijk is. Het hogere niveau 4 of zeer ernstig, is wanneer de dreiging ernstig en zeer nabij is. Verzoeker is van mening dat niveau 3 niet beantwoordt aan de noodzaak van 'werkelijk en actuele of voorzienbare bedreiging'. Ook beantwoordt het artikel niet aan de voorwaarde dat het bevel niet langer dan strikt noodzakelijk kan worden opgelegd. Er is in het artikel (met uitzondering van de automatische beëindiging bij gebrek aan KB binnen de maand voor maatregel op ganse grondgebied) niet voorzien hoe een einde wordt gemaakt aan het bevel.

E.4. Wat betreft artikel 126/3 §§ 3-5. bewaring in drie geografische zones onderscheiden door de aard van de dreiging

Verzoeker beoordeelt deze drie onderdelen van het artikel 126/3 samen en elk ook op zich.

90. E.4.1. Wettelijke bepalingen.

§ 3. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:

a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2, 3° tot 5°, van het Belgisch Scheepvaartwetboek;

b) de spoorwegstations in de zin van artikel 2, 5°, van de wet van 27 april 2018 op de politie van de spoorwegen;

c) de metro- en de pre-metrostations;

d) de luchthavens in de zin van artikel 2, punt 1), van Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden, met inbegrip van de luchthavens

die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU, alsook de entiteiten die de bijbehorende installaties bedienen welke zich op de luchthavens bevinden;

e) de gebouwen bestemd voor de administratie van douane en accijnzen;

f) de gevangenissen in de zin van artikel 2, 15°, van de basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van de gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gepleegd, bedoeld in artikel 606 van het Wetboek van strafvordering, en de forensisch psychiatrische centra, bedoeld in artikel 3, 4°, c), van de wet van 5 mei 2014 betreffende de internering;

g) de wapenhandelaars en schietstanden zoals bedoeld in artikel 2, 1° en 19°, van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens;

h) de inrichtingen bedoeld in artikel 3.1.a), van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;

i) de inrichtingen bedoeld in artikel 2, 1°, van het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;

j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de uitvoeringsbesluiten ervan; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;

k) de zetel van de NV Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en gecodeerde communicatie- en informatiesysteem bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

l) de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op basis van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

m) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.

§ 4. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, dit wil zeggen:

a) voor de openbare orde, de neutrale zones bedoeld in artikel 3 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten, en de ministeriële beleidscellen;

b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet

worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid wordt opgesteld op voorstel van de minister van Justitie en de minister van Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;

c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;

d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:

i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;

ii) de gemeentehuizen en de stadhuizen;

iii) het koninklijk paleis;

iv) de koninklijke domeinen;

v) de gebouwen toegewezen aan de instellingen bedoeld in titel III, hoofdstukken 5 tot 7 van de Grondwet;

vi) de gemeenten waar zich militaire domeinen bevinden;

vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;

e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;

f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid:

i) de ziekenhuizen bedoeld in artikel 2 van de gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;

ii) de Nationale Bank van België;

g) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.

§ 5. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, dit wil zeggen:

a) de ambassades en diplomatieke vertegenwoordigingen;

b) de gebouwen bestemd voor de Europese Unie;

c) de gebouwen en de infrastructuren bestemd voor de NAVO;

d) de instellingen van de Europese Economische Ruimte;

e) de instellingen van de Verenigde Naties;

f) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.

§ 6. Voor elke categorie van zone bedoeld in de paragrafen 3 tot 5, bepaalt de Koning de omvang van de perimeter van de zone.

Elke autoriteit die bevoegd is voor een van de aangelegenheden bedoeld in de paragrafen 3 tot 5, deelt jaarlijks op de door de Koning vastgestelde datum alleen aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de concrete vaststelling van de geografische zones.

Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten alleen deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld artikel 126/1, § 1, in deze zone zo spoedig mogelijk kan worden beëindigd.

Met uitzondering van de in paragraaf 4, b), bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten exclusief ter beschikking van het Vast Comité I wordt gesteld, stelt de door de Koning aangewezen dienst de bijgewerkte lijst van zones bedoeld in de paragrafen 3 tot 5 waar de gegevensbewaring verplicht is, ter beschikking van het Controleorgaan op de politionele informatie en van het Vast Comité I, elk binnen het kader van hun bevoegdheden.

Het Controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of het met redenen omklede bevel geven dat bepaalde geografische zones bedoeld in de paragrafen 3 tot 5, van de lijst geschrapt worden.

Op voorstel van de door de Koning aangewezen dienst stellen de minister van Defensie, de minister van Justitie, en de minister van Binnenlandse Zaken jaarlijks en bij elke wijziging bedoeld in het vijfde lid de lijst vast van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn.

Het ministeriële besluit bedoeld in het zesde lid wordt bekendgemaakt via vermelding in het Belgisch Staatsblad.

Na deze goedkeuring, zendt de door de Koning aangewezen dienst de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, naar de operatoren.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de gegevens die door de bevoegde autoriteiten aan de door de Koning aangewezen dienst worden meegedeeld of van de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, of zijn medewerking verleent aan de uitvoering van dit artikel, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

E.4.2. Systematisering van de wettelijke bepalingen

91. Het artikel betreft drie gebieden of zones die onderscheiden worden op basis van de aard van de bedreiging waaraan zij kunnen worden blootgesteld:

§3. Gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit.

§4. Zones waar er mogelijk ernstige bedreiging is voor de vitale belangen van land of de essentiële behoeften van de bevolking.

§5. Zones waar er mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen.

92. ***§3 Volgende gebieden worden weerhouden in het kader van bijzondere blootstelling aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit:***

a) de havenfaciliteiten, de havens en de havenbeveiligingszones;
b) de spoorwegstations;
c) de metro- en de pre-metrostations;
d) de luchthavens met inbegrip van de luchthavens die tot het kernnetwerk behoren, alsook de

entiteiten die de bijbehorende installaties bedienen welke zich op de luchthavens bevinden;
e) de gebouwen douane en accijnzen;
f) de gevangenissen, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gepleegd, en de forensische psychiatrische centra;
g) de wapenhandelaars en schietstanden;
h) de inrichtingen bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;
i) de inrichtingen betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;
j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;
k) de zetel van de NV Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en gecodeerde communicatie- en informatiesysteem bevinden betreffende de analyse van de dreiging;
l) de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van essentiële diensten ondersteunen;
m) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.

§4 Volgende zones worden weerhouden in het kader van een mogelijke ernstige bedreiging voor de vitale belangen van het land of de essentiële behoeften van de bevolking:

a) de neutrale zones en de ministeriële beleidscellen;
b) de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid;
c) de autosnelwegen en de bijhorende openbare parkeerterreinen;
d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:
i) de wetgevende vergaderingen;
ii) de gemeentehuizen en de stadhuizen;
iii) het koninklijk paleis;
iv) de koninklijke domeinen;
v) de gebouwen toegewezen aan Grondwettelijk Hof, Raad van State, Rechterlijke macht;
vi) de gemeenten waar zich militaire domeinen bevinden;
vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;
e) de grensgemeenten;
f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid:
i) de ziekenhuizen en andere verzorgingsinrichtingen;

ii) de Nationale Bank van België;
g) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.

§5. Volgende zones worden weerhouden in het kader van een mogelijk ernstige bedreiging voor de belangen van de op het nationaal grondgebied gevestigde internationale instellingen:

a) de ambassades en diplomatieke vertegenwoordigingen;
b) de gebouwen bestemd voor de Europese Unie;
c) de gebouwen en de infrastructuren bestemd voor de NAVO;
d) de instellingen van de Europese Economische Ruimte;
e) de instellingen van de Verenigde Naties;
f) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.

§ 6 van dit artikel 126/3 regelt bepaalde modaliteiten voor elke categorie van de zone bepaald in de paragrafen 3 tot 5.

93. Voor elke categorie wordt de perimeter van de zone bepaald door KB.

De voor de zone bevoegde autoriteit (de wet bepaalt niet wie dit specifiek is) deelt jaarlijks aan de door KB aangeduide dienst de gegevens mee voor vaststelling van de geografische zones.

Wanneer geografische zone niet langer beantwoordt aan het bedoelde criterium stelt de autoriteit die aangeduide dienst onverwijld in kennis zodat verplichting bewaring zo spoedig mogelijk kan worden beëindigd.

Op voorstel van die dienst stellen ministers van Defensie, Justitie en Binnenlandse Zaken jaarlijks en bij elke wijziging de lijst vast van geografische zones en hun bewaringstermijn.

94. E.4.3. Toepassing en discussie

E.4.3.1. Wat betreft het artikel 126/3 §§ 3-5 in het algemeen

95. Het HvJ verzet zich niet tegen gerichte bewaring op basis van een geografisch criterium, zoals plaatsen of infrastructuren die regelmatig door een zeer groot aantal personen wordt bezocht of strategisch plaatsen, bijvoorbeeld luchthavens, stations, zeehavens, tolzones. (SpaceNet, 108-110). Geografische zones kunnen en in voorkomend geval moeten worden gewijzigd (SpaceNet, 111). Niet langer dan strikt noodzakelijk in het licht van de nagestreefde doelstelling; verlenging mogelijk als noodzaak blijft bestaan (SpaceNet, 111). Eventuele moeilijkheden om tot nauwkeurige omschrijving te komen van gevallen en voorwaarden gerichte bewaring, rechtvaardigt niet dat van algemene en ongedifferentieerde bewaring de regel wordt gemaakt, in plats van de uitzondering (SpaceNet, 113). Maatregel moet passend en noodzakelijk zijn, en evenredig met het nagestreefde doel (SpaceNet, 122).

96. *In eerste instantie* wordt gesteld dat het groot aantal onderdelen van de onderscheiden plaatsen en infrastructuren die in het kader van gebieden en zones, waarbij de gegevens moeten bewaard worden, neerkomt op een bewaring van de gegevens op (quasi) het ganse Belgische grondgebied. Opgeteld gaat het om meer dan 45 onderscheiden plaatsen en infrastructuren. Maar de facto gaat het om honderden plaatsen en infrastructuren. Bijvoorbeeld de vermelding dat alle gemeentehuizen en alle lokalen van de politie, alle ambassades en diplomatieke posten, alle gerechtsgebouwen, alle wapenhandelaars, alle netwerken en informatiesystemen, alle autostrades enzovoort er onder vallen bevestigt dat er moeilijk nog een zone te vinden is in het land die niet onder de bewaarplicht zou vallen. Een objectieve toepassing op het Belgisch grondgebied van alle plaatsen en infrastructuren die geviseerd worden maakt duidelijk dat (wellicht) buiten de Hoge Venen en Park Hoge Kempen Limburg, het ganse grondgebied onder de verplichte bewaring valt. Reeds het betrekken van alle grensgemeenten maakt duidelijk dat reeds een essentieel groot onderdeel van het grondgebied betrokken wordt. Ook de opname van alle autosnelwegen, alle gemeentehuizen, alle hospitalen… maakt onmiskenbaar duidelijk dat in een klein land als België, het ganse grondgebied geviseerd is. Uit de parlementaire debatten is gebleken dat de regering op dit punt zelf die realiteit niet miskend heeft. Te buiten gelaten de (eventueel verantwoorde) situatie van een ernstige en zeer nabije dreiging (artikel 126/3 §2; niveau 4; zie hoger) komt dit neer op een algemene en ongedifferentieerde bewaring van gegevens van de ganse bevolking.

    Dit is nog des te meer problematisch omdat de perimeter voor de gebieden en zones niet bij wet is bepaald en door een KB zou bepaald worden, zonder dat in het KB een minimum- of maximumperimeter is opgenomen. Een perimeter van 5 kilometer geeft een andere realiteit dan een perimeter van 10 kilometer, maar verzoeker is van mening dat zelfs een minimale perimeter quasi het ganse grondgebied van het land kan insluiten.

97. *In tweede instantie* wordt gesteld dat de maatregelen met betrekking tot zones en gebieden het criterium dat op dit punt gehanteerd wordt door het HvJ ver te buiten gaat. Het HvJ neemt als criterium ‘plaatsen of infrastructuren waar het risico op het plegen of voorbereiden van zware criminaliteit bijzonder hoog is’, en verwijst naar ‘luchthavens, stations, zeehavens en tolzones.’ (SpaceNet, 108, 110). De regeling van artikel 126/3 §§3-5 omvat overwegend plaatsen en infrastructuren waarop dit criterium niet van toepassing is, zoals bijvoorbeeld gebouwen van de administratie van douane en accijnzen, forensische psychiatrische centra, inrichtingen ioniserende stralingen, alle gemeenten met meerdere kritische netwerken of infrastructuren, alle autowegen, alle gemeentehuizen en stadhuizen, alle grensgemeenten, ziekenhuizen en verzorgingsinstellingen, het gros van de internationale instellingen, enz…

    Voor die zones lijkt het niet voor de hand te liggen of ze al dan niet bestempeld kunnen worden als “plek waar veel zware criminaliteit plaatsvindt”, als “plaats waar er een verhoogd risico is op zware misdrijven, doordat ze regelmatig door een zeer groot aantal personen bezocht worden”, of nog als “strategische plek”. Dat is in ieder geval zo wat betreft, bijvoorbeeld, de autosnelwegen in hun geheel en de gemeentehuizen (advies Raad van State, Parl. St., Kamer, Doc 55 2572/001, p. 283). De huidige regeling inzake bewaring blijft aldus verre van beperkt tot het “strikt noodzakelijke”.

Zulks is trouwens ook een vaststelling die de GBA gedaan heeft, zeker wat betreft de Belgische autosnelwegen (advies GBA, Parl. St., Kamer, Doc 55 2572/001, p. 776).

Dat de doeltreffendheid van onderhavige regeling vooralsnog niet is bewezen (Parl. St., Kamer, Doc 55 2572/001, p. 78), toont des te meer aan dat de bestreden wet geen noodzakelijke maatregel betreft.

98. *Ten derde*, de zones van §4 vallen volgens de wet onder het begrip 'mogelijk ernstige bedreiging voor de vitale belangen van het land of de essentiële behoeften van de bevolking'. Deze kwalificatie valt niet onder de grondslagen op basis waarvan kan afgeweken worden van artikel 15, lid 1 van richtlijn 2002/58/EG, namelijk zware criminaliteit, ernstige bedreiging openbare veiligheid, bescherming nationale veiligheid, onbevoegd gebruik van elektronisch communicatiesysteem.

99. *Ten vierde,* maken de maatregelen met betrekking tot de zones dat er de facto een algemene bewaarplicht wordt ingesteld.

Zo bepaalt artikel 126/2 §3, alinea 1, j. de bewaring (van de gegevens bedoeld in artikel 126/1 §2, namelijk het bewaren door de operatoren van de gegevens van eindgebruikers van elektronische communicatiediensten) in gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meer kritieke infrastructuren bevinden. Deze kritieke infrastructuren omvatten ook datacenters. Dit impliceert dat de daar aanwezige servers getroffen worden, bijvoorbeeld deze van een ziekenhuis maar ook verhuurde servers in een commercieel datacenter of cloudproviders. Zij maken immers ook vaak verbinding met het internet via de operator. De uitbater van de dienst (bijvoorbeeld een bedrijf dat een server huurt in een datacenter met internetconnectie) is te beschouwen als de eindgebruiker van de connectie, en moet de verkeers- en locatiegegevens ervan moeten bewaard worden. Dit betekent dat ook effectieve dataretentie van al wie op afstand verbinding maakt met deze diensten in het kader van gebruik van die diensten. Aangezien zowat alle onlinediensten gebruik maken van verbindingen van het toestel van een natuurlijke-persoon-eindgebruiker naar een server, is de impact van een dergelijke dataretentie enorm en in de realiteit gelijk aan een algemene bewaarplicht. De dataretentie gebeurt dan niet aan het startpunt van de verbinding, maar aan het eindpunt. Maar de dataretentie treft quasi alle burgers. Deze enkele toepassing van één beperkt onderdeel van de bewaringsverplichting in het kader van gebieden blootgesteld aan bedreigingen tegen de nationale veilgiheid of voor het plegen van zware criminaliteit, toont aan dat het opnemen van een (op het eerste zicht) beperkte kritieke infrastructuur leidt tot de bewaring van gegevens met een zeer grote impact.

Zo worden ook personen die een vaste internetverbinding hebben en in de buurt wonen van bepaalde gebouwen of zones (bijvoorbeeld in de buurt van een station) getroffen door de dataretentie. Artikel 126/2 §2 heeft niet alleen betrekking op mobiele netwerken, maar in bepaalde onderdelen ook op vaste internetverbindingen. Het valt niet in te zien wat hiervan het nut is, aangezien de locatie van de vaste internetverbinding vaststaat en zich dus niet in het geviseerde gebouw (station…) bevindt. De nabijheid van deze vaste internetverbinding tot de zone heeft ook geen enkele relevantie wat betreft zware criminaliteit of nationale veiligheid.

E.4.3.2. Wat betreft de omvang van de perimeter voor wat betreft de zones bepaald bij artikel 126/3 §§3-5.

100. Artikel 126/3 §6 bepaalt dat de omvang van de perimeter voor de zones bedoeld in paragrafen 3 tot 5 bepaald worden bij KB. Ook deze bepaling is strijdig met het verbod op algemene en ongedifferentieerde bewaring, daar zij niet beantwoordt aan de vereiste van duidelijkheid en nauwkeurigheid. Er is in de wet niet eens bepaald welke minimale en maximale perimeters het KB zou moeten respecteren.

E.4.3.3. Wat betreft het in werking treden van de zones bepaald bij artikel 126/3 §§ 3-5.

101. Artikel 45 van de wet van 20 juli 2022 bepaalt dat de gerichte gegevensbewaring op basis van de criteria 126/3 §§ 3-5 in werking treden door KB en 'uiterlijk op 1 januari 2027'. Het betreft een datum die 3,5 jaar ligt na de stemming van de wet. Het bevestigt op zich de problematische toepassing van vermelde artikels en de afwezigheid van realiteitszin, daar er zoveel tijd nodig is om het systeem van gegevensbewaring, als het al zou kunnen werken, quod non, in vermelde zones in werking te kunnen stellen.

VI.4. VIERDE MIDDEL

Schending van artikel 11, 12, 22 en 29 Grondwet.

Schending van artikel 15, lid 1 en de artikels 5, 6 en 9 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), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8 , 11, 47 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

Schending van artikel 6, 8, 10, 11 en 18 van het Europees Verdrag voor de bescherming van de Rechten van de Mens (EVRM).

Schending van de artikels 13 en 54 van de Richtlijn 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Geschonden referentienormen.

Recht op eerbiediging van de persoonlijke levenssfeer en bescherming van persoonlijke data, al dan niet in samenhang gelezen met het recht op vertrouwelijkheid van communicatie en met de algemene beginselen van informatieve zelfbeschikking en de beginselen van noodzaak in een democratische samenleving, legaliteit, proportionaliteit en subsidiariteit.

Schending van de in het middel vermelde wettelijke bepalingen door artikel 127/1, dat door artikel 13 van de wet van 20 juli 2022 ingevoegd werd in de wet van 13 juni 2005 betreffende elektronische communicatie, inhoudend de bepalingen van de autoriteiten die gegevens mogen krijgen van de operatoren en de voorwaarden die hierbij in acht moeten worden genomen. De wettelijke regeling verleent toegang tot de bewaarde gegevens aan autoriteiten die niet onder de doelstellingen van artikel 15.1 e-Privacy Richtlijn 2002/58/EG vallen. Bovendien zijn de voorwaarden voor toegang niet in overeenstemming met vermeld artikel en met de rechtspraak HvJ

102. Dit vierde middel betreft de toegang tot de gegevens. Dit middel wordt in ondergeschikte orde geformuleerd daar zo de te bewaren gegevens een schending inhouden van de wettelijke bepalingen opgenomen in het eerste middel, de toegang op zich *de facto* zonder voorwerp is, en dus ook de bepalingen die de toegang bepalen moeten vernietigd worden. Voor wat betreft de logica, structuur, opbouw, referentiekaders en beoordelingsprincipes wordt verwezen naar en herhaald wat hierover onder het eerste middel is gesteld.

A. Aangevochten wettelijke bepaling

103. **Art. 127/1. § 1. Voor de toepassing van dit artikel omvat zware criminaliteit met name de feiten waarvoor er ernstige aanwijzingen bestaan:**

1° dat ze de minimale correctionele hoofdgevangenisstraf bedoeld in artikel 88bis, § 1, eerste lid, van het Wetboek van strafvordering tot gevolg kunnen hebben;

2° dat ze kunnen leiden tot een sanctie van niveau 5 of 6 zoals bedoeld in artikel XV.70 van het Wetboek van economisch recht;

3° dat ze een inbreuk zouden kunnen vormen op de artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (verordening betreffende machtsmisbruik) en houdende intrekking van Richtlijn 2003/6/EG van het Europees Parlement en de Raad en Richtlijnen 2003/124, 2003/125/EG en 2004/72/EG van de Commissie of op de bepalingen die worden genomen op basis of ter uitvoering van deze artikelen.

§ 2. Enkel de volgende autoriteiten mogen van een operator gegevens krijgen die worden bewaard krachtens de artikelen 122 en 123, voor de doeleinden hieronder voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm:

1° de inlichtingen- en veiligheidsdiensten, teneinde de opdrachten te volbrengen die hen worden toegewezen krachtens de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° de bevoegde autoriteiten met het oog op de voorkoming van ernstige bedreigingen voor de openbare veiligheid;

3° de autoriteiten belast met het vrijwaren van de vitale belangen van natuurlijke personen;

4° de autoriteiten bevoegd voor het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen;

5° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronische-communicatienetwerk of -dienst;

6° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat onder de zware criminaliteit valt;

7° de administratieve autoriteiten belast met het vrijwaren van een belangrijk economisch of financieel belang van de Europese Unie of van België, met inbegrip van de monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

8° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat een strafrechtelijke inbreuk vormt, maar niet onder de zware criminaliteit valt;

9° het Instituut in het kader van de controle van deze wet en de autoriteiten bevoegd voor de bescherming van de gegevens in het kader van hun controleopdrachten;

10° de autoriteiten die wettelijk gemachtigd zijn om data te hergebruiken voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden.

§ 3. De gegevens die worden bewaard krachtens de artikelen 126 en 127, worden bewaard voor de autoriteiten en de doeleinden bedoeld in paragraaf 2, 1° tot 8°.

Enkel de autoriteiten bedoeld in paragraaf 2 mogen van een operator gegevens ontvangen die

worden bewaard krachtens de artikelen 126 en 127, voor de doeleinden waarin dezelfde paragraaf voorziet, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

In afwijking van het tweede lid, mogen de in paragraaf 2, 10°, bedoelde autoriteiten van een operator geen aan de bron van de verbinding toegewezen IP-adressen krijgen.

In afwijking van het tweede lid, is een verzoek van een autoriteit om van een operator een IP-adres te krijgen dat is toegewezen aan de bron van een verbinding, enkel toegestaan voor de doeleinden van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventies van ernstige dreigingen tegen de openbare veiligheid en de vrijwaring van de vitale belangen van een fysieke persoon, wanneer die autoriteit in staat zou zijn om, met behulp van de informatie in haar bezit en de aan de bron van de verbinding toegewezen IP-adressen die ze van de operator heeft verkregen, het traject van een eindgebruiker op internet te achterhalen.

§ 4. De gegevens die worden bewaard krachtens de artikelen 126/1 en 126/3 worden bewaard voor de autoriteiten en doeleinden bedoeld in paragraaf 2, 1° tot 3° en 6°.

Enkel de in paragraaf 2, 1° tot 3°, 6° en 9°, bedoelde autoriteiten mogen van een operator voor de doeleinden beoogd in dezelfde paragraaf, de krachtens de artikelen 126/1 en 126/3 bewaarde gegevens krijgen, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

§ 5. De formele wettelijke norm van Belgisch recht bedoeld in de paragrafen 2 tot 4 preciseert:

- de categorie of categorieën van ondernemingen waaraan de autoriteit gegevens kan vragen;

- de categorieën van gegevens die mogen gevraagd worden;

- de beoogde doeleinden;

- de mechanismen ter controle van het verzoek om gegevens, die intern wordt uitgevoerd of, in voorkomend geval, door een rechterlijke instantie of door een onafhankelijke administratieve autoriteit.

De minister laat in het Belgisch Staatsblad een omzendbrief publiceren die een lijst omvat met de Belgische autoriteiten die gemachtigd zijn om van een operator gegevens te ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127.

Op het verzoek van de minister of van het Instituut verstrekken de Belgische autoriteiten bedoeld in de paragrafen 2 tot 4 de informatie die nodig is om deze omzendbrief op te stellen.

§ 6. De verzoeken die de autoriteiten richten aan de operatoren om bepaalde gegevens te verkrijgen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 of 127, omvatten de volgende minimale vermeldingen:

1° de identiteit van de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de identiteit van die dienst;

2° de functie van de contactpersoon bij de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de functie van de contactpersoon bij die centrale dienst;

3° de juridische grondslag waarop het verzoek gebaseerd is, behalve wanneer het verzoek naar de operator wordt verzonden via een centrale dienst voor rekening van een andere autoriteit;

4° de gewenste antwoordtermijn.

§ 7. Het Instituut stuurt jaarlijks aan de minister en de minister van Justitie statistieken over de verstrekking aan de autoriteiten van gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127. Deze ministers sturen die jaarlijks door naar de Kamer van

volksvertegenwoordigers.

Die statistieken omvatten met name:

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

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

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

Die statistieken mogen geen persoonsgegevens noch vertrouwelijke informatie omvatten.

De gegevens die betrekking hebben op de toepassing van het tweede lid, 1°, worden tevens bijgevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90decies van het Wetboek van strafvordering uitbrengt aan het Parlement.

Het Instituut vraagt aan de operatoren en aan de door de Koning aangewezen dienst de informatie aan de hand waarvan het de in het eerste lid bedoelde verplichting kan vervullen.

B. Systematisering van artikel 127/1

104. De essentie van het artikel (§2) betreft de autoriteiten die gegevens, bewaard krachtens artikel 122 en 123, mogen opvragen bij de operatoren bepaald door en onder voorwaarden vastgelegd in een formele wettelijke norm.

105. *In eerste instantie* wordt onderlijnd dat tien onderscheiden autoriteiten toegang tot de bewaarde gegevens kunnen hebben:

1° de inlichtingen- en veiligheidsdiensten;

2° de bevoegde autoriteiten met het oog op de voorkoming van ernstige bedreigingen voor de openbare veiligheid;

3° de autoriteiten belast met het vrijwaren van de vitale belangen van natuurlijke personen;

4° de autoriteiten bevoegd voor het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen;

5° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronische-communicatienetwerk of -dienst;

6° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat onder de zware criminaliteit valt;

7° de administratieve autoriteiten belast met het vrijwaren van een belangrijk economisch of financieel belang van de Europese Unie of van België, met inbegrip van de monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

8° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat een strafrechtelijke inbreuk vormt, maar niet onder de zware criminaliteit valt;

9° het Instituut in het kader van de controle van deze wet en de autoriteiten bevoegd voor de bescherming van de gegevens in het kader van hun controleopdrachten;

10° de autoriteiten die wettelijk gemachtigd zijn om data te hergebruiken voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden.

106. *In tweede instantie (§1)* geeft het artikel een invulling van 'zware criminaliteit' in het kader van de toepassing van het artikel zelf; deze invulling betreft enkel op de bevoegde autoriteit vermeld onder 6°. Het artikel geeft een andere invulling aan het begrip 'zware criminaliteit' dan deze van artikel 90ter §§2 tot 4 wetboek strafvordering, bepaald in artikel 126/3 §1 dat betrekking heeft op het bepalen van de zones waar op basis van criminaliteitscijfers bewaring wordt opgelegd.

107. *In derde instantie* wordt aangeduid welke autoriteit welke gegevens kan opvragen.

De tien autoriteiten van § 2 mogen de gegevens opvragen die krachtens artikel 122 en 123 bewaard worden. Dit betreft een zeer ruime waaier van verkeersgegevens die operatoren voor facturering, marketing, fraude en kwaadwillig gebruik netwerk (122) bewaren of locatiegegevens die operatoren voor de veiligheid van het netwerk (123) bewaren. De gegevens bewaard door artikel 126 en 127 kunnen 'enkel' door de autoriteiten §2, 1° tot 8° opgevraagd worden. Die gegevens betreffen eveneens een zeer ruim pakket: 17 specifieke gegevens (126) en een veertigtal vooral identificatiegegevens (127). De gegevens bewaard door artikel 126/1 en 126/3 mogen 'enkel' door de autoriteiten §2, 1° tot 3° en 6° worden opgevraagd. Het betreft de gegevens bewaard op basis van geografische zones (126/1) en een tiental specifieke identificatiegegevens (126/2).

108. *In vierde instantie* bepaalt paragraaf 5 wat de formele norm bedoeld in paragrafen 2 tot 4 moet preciseren: categorie ondernemingen, categorie gegevens, doeleinden, controlemechanismen. Die paragraaf bepaalt dat de minister (welke?) in het Belgisch Staatsblad een omzendbrief publiceert met de lijst van de Belgische autoriteiten die gemachtigd zijn van de operatoren gegevens te ontvangen die bewaard zijn op basis van 122, 123, 126, 126/1, 126/3 en 127.

C. Het standpunt van het HvJ in verband met de toegang tot de gegevens

109. De vermelde arresten van het HvJ hebben zich bijna uitsluitend uitgesproken over de bewaring van de gegevens. Daar deze arresten in La Quadrature du Net en SpaceNet gesteld hebben dat de bepalingen in respectievelijk de Franse, Britse en Belgische dataretentiewetten, en in de Duitse dataretentiewet niet beantwoorden aan de bewaringsvereisten, sprak het HvJ zich slechts zeer beperkt uit over de toegang. Dit laatste was niet de kern van de gestelde prejudiciële vragen.

110. In de marge van die discussie heeft het HvJ zich in de zaken Commissioner en SpaceNet wel uitgesproken over de toegang tot algemeen en ongedifferentieerde bewaarde gegevens. Er was immers opgeworpen dat de waarborgen met betrekking tot de toegang tot de gegevens voldoende verhielp en een voldoende beperking oplegde aan de inmenging in de rechten in het kader van de bewaring. Het HvJ verwierp dit standpunt en stelde dat bewaring en toegang twee onderscheiden inmengingen zijn die een verschillende rechtvaardiging vereisen. (perscommuniqué nr. 156/22 HvJ 20 september 2022)

> 128 Zoals het Hof reeds heeft geoordeeld, kan de **toegang** tot verkeers- en locatiegegevens die door aanbieders van elektronische-communicatiediensten worden bewaard op grond van een krachtens artikel 15, lid 1, van richtlijn 2002/58 getroffen maatregel – welke toegang moet

worden verleend met volledige inachtneming van de voorwaarden die voortvloeien uit de rechtspraak waarin deze richtlijn is uitgelegd – **in beginsel enkel worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop die bewaringsverplichting aan die aanbieders is opgelegd.** De zaak ligt slechts anders wanneer de met de toegang nagestreefde doelstelling belangrijker is dan die welke de bewaring rechtvaardigde (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 98).

129 Het betoog van de Deense regering ziet echter op een situatie waarin de doelstelling van het bedoelde toegangsverzoek, te weten het bestrijden van zware criminaliteit, in de hiërarchie van doelstellingen van algemeen belang minder belangrijk is dan de doelstelling die de bewaring rechtvaardigde, te weten de bescherming van de nationale veiligheid. In die situatie toegang verlenen tot de bewaarde gegevens zou indruisen tegen de in het vorige punt alsook in de punten 68, 71, 72 en 73 van het onderhavige arrest in herinnering gebrachte hiërarchie van doelstellingen van algemeen belang (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 99).

130 Bovendien en vooral mogen verkeers- en locatiegegevens volgens de in punt 74 van het onderhavige arrest in herinnering gebrachte rechtspraak niet algemeen en ongedifferentieerd worden bewaard met het oog op de bestrijding van zware criminaliteit, zodat het verlenen van toegang tot die gegevens voor datzelfde doel niet gerechtvaardigd kan zijn. Wanneer die gegevens bij wijze van uitzondering onder de in punt 71 van dit arrest vermelde voorwaarden algemeen en ongedifferentieerd zijn bewaard om de nationale veiligheid te beschermen tegen een bedreiging die reëel en actueel of voorzienbaar is, mogen de nationale autoriteiten die bevoegd zijn voor strafonderzoeken, in het kader van strafvervolging geen toegang tot die gegevens hebben, omdat anders het in punt 74 van het onderhavige arrest in herinnering gebrachte verbod op een dergelijke bewaring met het oog op de bestrijding van zware criminaliteit elk nuttig effect zou verliezen (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 100).

D. <u>Toepassing en discussie</u>

111. De rechtspraak van het HvJ houdt in dat de toegang op zich een rechtvaardiging vereist vanuit de bescherming van de nationale veiligheid, de bestrijding van de zware criminaliteit… En dat wanneer gegevens bewaard werden op de grondslag van de nationale veiligheid er geen toegang kan zijn op de grondslag van de zware criminaliteit.

112. De autoriteiten die toegang krijgen zijn veel ruimer en de meesten van hen vallen buiten het kader van de grondslagen waarop gegevens mogen bewaard worden en dus waartoe dan in tweede instantie toegang kan verleend worden.

De grondslagen voor databewaring van artikel 15 lid 1 e-Privacy Richtlijn – nationale veiligheid, openbare veiligheid, zware criminaliteit, strafbaar of onbevoegd gebruik elektronisch communicatiesysteem – zijn niet de bevoegdheid van de autoriteiten vermeld onder 3°, 5°, 7°, 8° 9°

van § 2 van artikel 127/1 die toegang kunnen vragen. Aan hen kan dan ook geen toegang verleend worden. Er is geen conforme artikel 15 lid 1 rechtvaardiging voor hun toegang tot de gegevens.

113. Artikel 127/2 maakt tien onderscheiden autoriteiten met diverse bevoegdheden bevoegd om toegang tot de gegevens te krijgen. De eerste data retentiewet van 30 juli 2013 beperkte in artikel 5§ 2 de bewaring van de gegevens 'met het oog op' de handelingen voor vier doeleinden (opsporing…strafbare feiten; taken inlichtingendiensten; onderzoek Ombudsdienst telecommunicatie; beteugeling kwaadwillige oproepen naar nooddiensten). De tweede data retentiewet van 29 mei 2016 machtigde in artikel 4, zes autoriteiten de toegang tot gegevens. Van deze zes zijn enkel de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten behouden. De acht andere autoriteiten zijn nieuw. Terwijl de tweede dataretentiewet werd vernietigd met de motivering dat het arrest van het Hof van Justitie van 6 oktober 2020 'een verandering van gezichtspunt oplegde ten opzichte van de keuze die de wetgever heeft gemaakt', en 'dat de inmenging moet waarborgen dat zij tot het strikt noodzakelijke wordt beperkt' (arrest nr. 57/2021 GwH 22 april 2021, B.18) doet de wetgever in deze derde dataretentiewet precies het omgekeerde en maakt hij de inmenging nog breder, door de grote uitbreiding van de autoriteiten die toegang kunnen krijgen.

114. Ook de beperking voor bepaalde autoriteiten tot bepaalde bewaarde gegevens is geen rechtvaardiging voor de toegang. De toegang betreft een breed spectrum van gegevens. Zo hebben de autoriteiten van §2, 1 tot en met 10 (dus alle vermelde autoriteiten) toegang tot de (zeer ruime) gegevens van artikels 122 en 123; de autoriteiten van §2, 1 tot en met 8 bovendien ook toegang tot de (nog ruimere) gegevens van artikel 126 en 127; de autoriteiten van §2, 1° tot 3° en 6° en 9° bijkomend toegang tot (eveneens ruime) gegevens van artikels 126/1 en 126/3.

115. De invulling van het begrip 'zware criminaliteit'(§1) 'in het kader van de toepassing van het artikel zelf', slaat enkel op de autoriteit vermeld onder 6°. Het artikel geeft een andere invulling aan het begrip 'zware criminaliteit' dan deze van artikel 90ter §§2 tot 4 wetboek strafvordering, bepaald in artikel 126/3 §1 dat betrekking heeft op het bepalen van de zones waar op basis van criminaliteitscijfers bewaring wordt opgelegd. Paragraaf 1, 1° artikel 127/1 hanteert als criterium om de vermelde autoriteit bevoegd te verklaren om gegevens op te vragen dat er 'ernstige aanwijzingen bestaan' dat het gaat om feiten 'die een minimale gevangenisstraf bedoeld in artikel 88bis §1, eerste lid wetboek strafvordering tot gevolg kunnen hebben'. Vermeld artikel betreft een correctionele hoofdgevangenisstraf van één jaar of zwaarder. Ook de invoering van het begrip 'ernstige aanwijzingen' is in dit kader problematisch. Het is duidelijk dat deze bepaling niet beantwoordt aan het begrip 'zware criminaliteit'. Het gaat om een veel breder criterium dan artikel 90ter §§2 tot 4. Een zeer breed scala van misdrijven valt onder dat begrip. Er is in dezelfde wet een *duidelijke tegenspraak* tussen wat in het kader van de bewaring en in het kader van de toegang onder het begrip 'zware criminaliteit' verstaan wordt.

116. Deze bepaling van 'zware criminaliteit' schendt artikel 15 lid 1 e-Privcay richtlijn die enkel op grondslag van zware criminaliteit bewaring, en ook toegang tot gegevens toelaat, ook voor de administratieve of gerechtelijke autoriteiten bevoegd voor preventie, onderzoek, opsporing of vervolging van een feit dat onder zware criminaliteit valt. Ook het begrip administratieve autoriteit die ter zake zware criminaliteit zou bevoegd zijn is problematisch. Te buiten gelaten de inlichtingen- en veiligheidsdiensten, met hun

specifieke bevoegdheden, is het de vraag welke administratieve autoriteit bevoegd is voor zware criminaliteit. Voor de inlichtingen- en veiligheidsdiensten is er een eigen bepaling in artikel 127/1 §2.

117. De toegang door de autoriteit bepaald in §2, 8° valt volledig buiten de doelstellingen die op basis van artikel 15 lid 1 ePrivacy richtlijn een inmenging mogelijk maken. Het betreft de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een *feit dat een strafrechtelijk inbreuk vormt, maar niet onder zware criminaliteit valt.* De tekst is duidelijk: het gaat om alle strafrechtelijke inbreuken die niet onder zware criminaliteit vallen. De wet bepaalt op dat punt geen enkele beperking. Het gaat dus om alle strafbare feiten gaande van een verkeersinbreuk tot sluikstorten, enz… Het gaat om een toegang tot de gegevens van de artikelen 122, 123, 126 en 127, bijgevolg een zeer ruime waaier van gegevens bewaard door de operatoren. Bovendien beperkt deze bevoegdheid zich niet tot de gerechtelijke autoriteiten maar ook tot de administratieve autoriteiten. Een burgemeester kan bij wijze van voorbeeld vermelde gegevens opvragen als hij van mening is dat er een strafrechtelijke inbreuk, die niet onder zware criminaliteit valt, op zijn grondgebied plaats heeft gevonden.

118. Er wordt in paragraaf 5 van artikel 127/1 verwezen naar de 'formele wettelijke norm' bedoeld in paragrafen 2 tot 4. In die paragrafen wordt gesteld dat de autoriteiten toegang hebben bepaald door en onder voorwaarden vastgesteld in een formele wettelijke norm. Paragraaf 5 bepaalt enkel wat de formele norm moet preciseren, maar duidt niet aan welke nu precies die formele norm is die bedoeld is in de paragrafen 2 tot 4. Met andere woorden: op basis van welke formele wettelijke norm hebben ieder van die tien bevoegde autoriteiten toegang tot de bewaarde gegevens? Voor alle duidelijkheid: de formele wettelijke norm moet een specifieke norm zijn die de voorwaarden voor toegang per categorie van autoriteit moet bepalen. Uit de tekst van de wet kan niet afgeleid worden dat een dergelijke wettelijke norm effectief bestaat.

119. Verder wordt in paragraaf 5 van artikel 127/1 gesteld dat de minister in het Belgisch Staatsblad een omzendbrief publiceert met de lijst van de Belgische autoriteiten die bevoegd zijn van een operator gegevens te ontvangen die bewaard worden krachtens artikelen 122, 123, 126, 126/1, 126/3 en 127. Te buiten gelaten dat niet wordt aangeduid welke de bevoegde minister hiervoor is, wordt opgemerkt dat een omzendbrief niets kan wijzigen aan de vermelde wettelijke bepalingen die op precieze wijze de bevoegde autoriteiten aanduiden.

VI.5. VIJFDE MIDDEL

Geschonden wetsartikels en referentienormen

Schending van artikel 10, 11, 22 en 29 Grondwet op zich of in samenlezing met de onderstaande artikels.

Schending van artikel 15, lid 1 en de artikels 5, 6 en 9 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), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

Schending van artikel 6, 8, 10, 11 en 18 van het Europees Verdrag voor de bescherming van de Rechten van de Mens (EVRM).

Schending van de artikels 13 en 54 van de Richtlijn 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Geschonden referentienormen.

Bescherming van het beroepsgeheim van advocaten, artsen en journalisten. Recht op eerbiediging van de persoonlijke levenssfeer en bescherming van persoonlijke data, al dan niet in samenhang gelezen met het recht op vertrouwelijkheid van communicatie en met de algemene beginselen van informatieve zelfbeschikking en de beginselen van noodzaak in een democratische samenleving, legaliteit, proportionaliteit en subsidiariteit.

De wettelijke regeling voert een algemene en ongedifferentieerde bewaring in van de gegevens. De wettelijke regeling maakt geen differentiëring wat betreft de gegevens die beschermd zijn door het beroepsgeheim zoals advocaten, artsen en journalisten. De wettelijke regeling verleent aan tien verschillende autoriteiten toegang tot de gegevens bewaard bij advocaten, artsen en journalisten.

120. Voor wat betreft de strijdigheid van de wettelijke regeling in verband met de bewaring van gegevens door de operatoren en de bewaring in geografische zones, en in verband met de toegang tot de gegevens, verwijst verzoeker naar de hogervermelde middelen. Deze middelen hebben de vernietiging van alle bepalingen van de wet van 20 juli 2022 als consequentie. Dit specifieke middel met betrekking tot advocaten, artsen en journalisten wordt in ondergeschikte orde ontwikkeld.

121. Het arrest HvJ SpaceNet van 20 september 2022 stelt dat de Duitse TKG-wet strijdig is met artikel 15.1 Richtlijn 2002/58/EG en de artikelen 7 en 8 van het Handvest Grondrechten EU, waar de wet een algemene bewaring van gegevens van advocaten en artsen toelaat (punt 82). Het arrest stelt dat bewaring en toegang onderscheiden inmengingen zijn die een verschillende rechtvaardiging vereisen (punt 91):

> 82 Bovendien heeft de Duitse regering in antwoord op een ter terechtzitting gestelde vraag gepreciseerd dat slechts **1 300 entiteiten waren opgenomen op de lijst van personen, instanties of organisaties van sociale of godsdienstige aard** waarvan de gegevens over elektronische communicatie op grond van § 99, lid 2, en § 113b, lid 6, TKG **niet worden bewaard**, hetgeen onmiskenbaar een **beperkt aantal** is ten opzichte van alle gebruikers van telecommunicatiediensten in Duitsland van wie de gegevens wel vallen onder de bewaringsverplichting die wordt opgelegd bij de in de hoofdgedingen aan de orde zijnde nationale regeling. **Zo worden onder meer de gegevens van aan het beroepsgeheim onderworpen gebruikers, zoals advocaten, artsen en journalisten, bewaard.**
>
> 91 Wat in de **derde plaats de waarborgen** betreft waarin de in de hoofdgedingen aan de orde zijnde nationale regeling voorziet en die ertoe strekken de bewaarde gegevens te **beschermen tegen de risico's op misbruik en tegen elke onrechtmatige toegang,** zij opgemerkt dat de **bewaring van deze gegevens en de toegang** ertoe – zoals blijkt uit de in punt 60 van het onderhavige arrest in herinnering gebrachte rechtspraak – **onderscheiden inmengingen** in de door de artikelen 7 en 11 van het Handvest gewaarborgde grondrechten vormen waarvoor een **verschillende rechtvaardiging vereist** is op grond van artikel 52, lid 1, van het Handvest. Derhalve kan een nationale wettelijke regeling die zorgt voor de volledige naleving van de voorwaarden die voortvloeien uit de rechtspraak waarbij richtlijn 2002/58 is uitgelegd op het gebied van de toegang tot de bewaarde gegevens, per definitie de ernstige inmenging in de door de artikelen 5 en 6 van deze richtlijn gewaarborgde rechten en in de grondrechten waarvan deze artikelen de concretisering vormen, beperken noch verhelpen (arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punt 47).

122. Het HvJ bevestigt hiermee haar rechtspraak dat, bij bewaring van gegevens, een nuttig onderscheid dient gemaakt te worden tussen personen van wie de communicatie onderworpen is aan het beroepsgeheim en de andere personen. (HvJ, Tele2Sverige, arrest van 21 december 2016, C-203/15).

De regeling ingesteld door de hier bestreden wet van 20 juli 2022 behandelt de bewaring van de communicatiedata van personen onderworpen aan het beroepsgeheim op identieke wijze als deze van personen die niet onderworpen zijn aan het beroepsgeheim. Er is in de wet geen enkel pertinent controlemechanisme voorzien dat de personen die genieten van het beroepsgeheim toelaat zich te verzetten tegen de verzameling, bewaring of kennisname van hun gegevens. Categorieën van personen die zich objectief gesproken in een onderscheiden situatie bevinden, kunnen niet op dezelfde manier behandeld worden. De maatregel die geen onderscheid maakt op basis van categorieën van personen die zich om redenen van hun beroepsgeheim in een onderscheiden situatie bevinden, is niet proportioneel in verhouding tot het nagestreefde doel;

Zowel in de door de operatoren te bewaren gegevens, als in de gegevens die op basis van geografische criteria te bewaren zijn, wordt er geen onderscheid gemaakt tussen personen beschermd door het beroepsgeheim en de andere personen.

123. Advocaten zijn beschermd door het beroepsgeheim. Verzoeker verwijst naar wat in het verzoekschrift van l'Ordre des Barreaux francophones et germanophone (Avocat.be) ontwikkeld is onder het punt 4.2.1. (pp. 52-56).

Verzoeker sluit zich aan bij de vier onderdelen die door Avocat.be ontwikkeld zijn in vermeld verzoekschrift. De maatregel (1) maakt geen onderscheid tussen gebruikers van de communicatie die beschermd zijn door het beroepsgeheim, en de andere gebruikers, (2) maakt geen onderscheid tussen de gegevens die door het beroepsgeheim gedekt zijn, en andere gegevens, (3) voert opnieuw een veralgemeende bewaring van de gegevens van het geheel van de burgers in, (4) is niet proportioneel in verhouding tot het nagestreefde doel.

124. Verzoeker wijst nog bijkomend op het volgende. Het gewijzigde artikel 88bis van het wetboek van strafvordering betreft de specifieke maatregel van het opsporen en lokaliseren en toegang door de onderzoeksrechter van gegevens in geval er ernstige aanwijzingen zijn van een strafbaar feit. De maatregel kan betrekking hebben op een advocaat of arts die zelf verdacht wordt van een strafbaar feit. Bij de tenuitvoerlegging wordt de stafhouder of vertegenwoordiger van de provinciale orde van geneesheren op de hoogte gebracht en wat onder het beroepsgeheim valt wordt niet opgenomen in het proces-verbaal. Deze maatregel van specifieke bewaring en toegang is ruim onvoldoende om de ongrondwettigheid van de algemene bewaring zelf van de gegevens ongedaan te maken. Deze maatregel heeft verder geen betrekking tot de (negen) andere autoriteiten die op zich ook de toegang kunnen vragen tot de gegevens van advocaten, artsen en journalisten.

OM DEZE REDENEN,

En alle in de loop van het geding te doen gelden redenen,

Behage het het Grondwettelijk Hof,

De wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten (bekend gemaakt in het Belgisch Staatsblad van 8 augustus 2022) in zijn geheel te vernietigen.

Brussel, 6 februari 2023

Voor verzoeker

Zijn raadsman

Mr Raf Jespers

Inventaris van de stukken

1. De wet van 20 juli 20222022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten (bekend gemaakt in het Belgisch Staatsblad van 8 augustus 2022)
2. Mandaat van de Liga voor Mensenrechten
3. Statuten VZW Liga voor Mensenrechten