| | | |
|---|---|---|
| Datum van inontvangstneming | : | 02/12/2024 |

**Zaak C-661/24**

**Samenvatting van het verzoek om een prejudiciële beslissing overeenkomstig artikel 98, lid 1, van het Reglement voor de procesvoering van het Hof van Justitie**

**Datum van indiening:**

9 oktober 2024

**Vewijzende rechter:**

Grondwettelijk Hof (België)

**Datum van verwijzingsbeslissing:**

26 september 2024

**Verzoekende partijen:**

Ordre des barreaux francophones et germanophone

Académie Fiscale ASBL

UA

Liga voor Mensenrechten VZW

Ligue des droits humains ASBL

JU

LV

Ministry of Privacy

**Verwerende partij:**

Premier ministre/Eerste Minister

---

**Voorwerp van de procedure in het hoofdgeding**

Beroepen tot gehele of gedeeltelijke 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 (hierna: „bestreden wet”) in vijf gevoegde zaken die respectievelijk op 4 januari 2023 en 6, 7, 8 en 9 februari 2023 zijn ingeleid door, ten eerste, de Ordre des barreaux francophones et germanophone (verzoek om vernietiging van artikel 5, punten 4 en 6, de artikelen 8-11, 13-15, 19, 21, 22, 24-42 en 44), ten tweede, de ASBL „Académie Fiscale” en UA (verzoek om vernietiging van de artikelen 2-17), ten derde, de VZW „Liga voor Mensenrechten”, ten vierde, de ASBL „Ligue des droits de l'Homme” en, ten vijfde, JU, de private stichting „Ministry of Privacy” en LV (deze laatste drie verzoeken strekken tot gehele vernietiging van de bestreden wet).

## Belangrijkste aangevoerde bepalingen van Unierecht en internationaal recht

### *Europees Verdrag tot Bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: „EVRM”)*

Artikel 6 – Recht op een eerlijk proces

Artikel 8 – Recht op eerbiediging van privé-, familie- en gezinsleven

„1. Eenieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.”

Artikel 10 – Vrijheid van meningsuiting

„1. Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen. [...]

2. Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen.”

Artikel 18 – Inperking van de toepassing van beperkingen op rechten

***Handvest van de grondrechten van de Europese Unie (hierna: „Handvest")***

Artikel 7

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

Artikel 8

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

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

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

Artikel 11

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

[...]"

Artikel 47 – Recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht

Artikel 52

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

[...]

3. Voor zover dit Handvest rechten bevat die corresponderen met rechten welke zijn gegarandeerd door het [EVRM], zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend. Deze bepaling verhindert niet dat het recht van de Unie een ruimere bescherming biedt.

[...]"

***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) (hierna: „richtlijn 2002/58/EG")***

Artikel 5 – Vertrouwelijk karakter van de communicatie

Artikel 6 – Verkeersgegevens

(verwerking van verkeersgegevens met name voor de opsporing van fraude)

Artikel 9 – Andere locatiegegevens dan verkeersgegevens

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

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

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

Artikel 15, lid 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 elektronischecommunicatiesysteem 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 [Unierecht], met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie."

***Richtlijn (EU) 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 [hierna: „richtlijn (EU) 2016/680"]***

Artikel 13 – Aan de betrokkene ter beschikking gestelde of verstrekte informatie

Artikel 54 – Recht om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke of een verwerker

***Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming) (hierna: „AVG")***

Artikel 23 – Beperkingen

**Belangrijkste aangevoerde nationale bepalingen**

***Belgische Grondwet (hierna „Grondwet")***

Artikel 10 (gelijkheidsbeginsel)

Artikel 11 (non-discriminatiebeginsel)

Artikel 12 (persoonlijke vrijheid)

Artikel 15 (onschendbaarheid van de woning)

Artikel 22

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

[...]”

**Korte uiteenzetting van de feiten en de procedure in het hoofdgeding**

1 De bestreden wet is een „reparatiewet”, die strekt tot naleving van de beginselen die gelden voor de bescherming van persoonsgegevens nadat de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie (hierna: „vernietigde wet”) in een eerder arrest van het Grondwettelijk Hof nr. 57/2021 van 22 april 2021 (ECLI:BE:GHCC:2021:ARR.057, hierna: „vernietigingsarrest”) was vernietigd.

2 Dit vernietigingsarrest is gewezen nadat het Grondwettelijk Hof aan het Hof van Justitie (hierna: „Hof” of „HvJ”) prejudiciële vragen heeft gesteld die 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, hierna: „arrest Quadrature du Net”), hebben geleid.

3 Met de bestreden wet heeft de wetgever ook willen reageren op de vernietiging in het arrest van het Grondwettelijk Hof nr. 158/2021 van 18 november 2021 (ECLI:BE:GHCC:2021:ARR.158) van de wet van 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, omdat op grond van artikel 22 van de Grondwet (eerbiediging van het privéleven) verzamelde gegevens en documenten in de wet dienen te worden opgesomd.

4 De vernietigde wet voorzag met name in de verplichting voor aanbieders van openbare telefoniediensten, via internet inbegrepen, van internettoegang, en van e-mail via het internet, om bepaalde categorieën locatie- en verkeersgegevens gedurende een periode van twaalf maanden te bewaren, opdat deze gegevens beschikbaar zouden zijn voor doeleinden van rechtshandhaving (strafrechtelijk onderzoek) dan wel voor de vervulling van opdrachten van de inlichtingendiensten.

5 Bij deze gegevens gaat het niet om de inhoud van de communicatie. Daarom worden zij „metagegevens” genoemd (bijvoorbeeld „wie belt wie”).

6 De vernietigde wet voorzag in een verplichting tot algemene en ongedifferentieerde bewaring van bepaalde metagegevens.

7 In zijn vernietigingsarrest heeft het Grondwettelijk Hof na het arrest Quadrature du Net geoordeeld dat „de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie de uitzondering moet zijn, en niet de regel”.

8 In het dictum van het arrest Quadrature du Net, heeft het Hof voor recht verklaard:

„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], 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], verzet zich daarentegen niet tegen wettelijke maatregelen

– die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten 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 elektronischecommunicatiemiddelen, 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 elektronischecommunicatiediensten 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."

9 In het vernietigingsarrest heeft het Grondwettelijk Hof geoordeeld dat het aan de wetgever staat een nieuwe regeling voor de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie tot stand te brengen waarbij de beginselen in acht worden genomen die op dit gebied van toepassing zijn, in het licht van de rechtspraak van het Hof met betrekking tot artikel 15, lid 1, van richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11 en 52, lid 1, van het [Handvest].

10 De vernietigde wet is er derhalve op gericht om de eisen van de rechtspraak voor de bescherming van persoonsgegevens ten uitvoer te leggen.

**Voornaamste argumenten van partijen in het hoofdgeding en analyse van het Grondwettelijk Hof**

11 Met betrekking tot de 14 grieven die door de verzoekende partijen tegen de bestreden wet zijn aangevoerd, heeft het Grondwettelijk Hof geoordeeld dat alleen de bezwaren over de volgende punten twijfels doen rijzen over de uitlegging van het Unierecht:

1) De bewaring van verkeersgegevens;

2) De bewaring van locatiegegevens, en

3) De bevoegdheden van de officieren van gerechtelijke politie van het BIPT (Belgisch Instituut voor postdiensten en telecommunicatie, regulator van de Belgische post- en telecommunicatiesector).

12 Deze grieven worden in de aangegeven volgorde uiteengezet.

***Bewaring van verkeersgegevens (artikel 5 van de bestreden wet)***

13 Artikel 5, punt 4, van de bestreden wet wijzigt artikel 122, paragraaf 4, van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna: „wet van 13 juni 2005") als volgt:

„§ 4. In afwijking van paragraaf 1 [beginsel van het wissen van verkeersgegevens van abonnees zodra deze niet langer nodig zijn voor de transmissie van de communicatie], teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, [dat bepaalt: „Zonder kennis te nemen van de inhoud van de communicatie, treffen de operatoren de gepaste, evenredige, preventieve en curatieve maatregelen, rekening houdende met de meest recente technische mogelijkheden, om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen en om te vermijden dat de eindgebruikers schade lijden of lastiggevallen worden."] 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 [BIPT] 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.”

14 Artikel 5, punt 5, van deze wet voegt aan artikel 122 van de wet van 13 juni 2005 een paragraaf 4/1 toe die als volgt luidt:

„§ 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 elektronischecommunicatienetwerken 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 elektronischecommunicatienetwerken en -diensten, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de schending van de veiligheid van hun elektronischecommunicatienetwerken en -diensten doorsturen.”

*Standpunt van partijen*

15 Verzoekende partij in de derde zaak laakt dat bovenvermelde bepalingen een algemene en ongedifferentieerde bewaring van communicatiegegevens instellen, zonder dat die bewaring noodzakelijk en strikt beperkt is ten aanzien van het nagestreefde doel, hetgeen in strijd is met de artikelen 11, 12, 22 en 29 van de Grondwet (waarin respectievelijk het non-discriminatiebeginsel, het recht op persoonlijke vrijheid, het recht op eerbiediging van het privéleven en het recht op de onschendbaarheid van het briefgeheim zijn neergelegd), artikel 15, lid 1, en de artikelen 5, 6 en 9 van richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, de artikelen 6, 8, 10, 11 en 18 van het EVRM en de artikelen 13 en 54 van richtlijn (EU) 2016/680.

16 Zij voegt eraan toe dat het doel, zijnde de goede werking van de netwerken en de diensten, niet in artikel 23 AVG (dat een beperking van de rechten toelaat) wordt vermeld, zodat de maatregel niet toelaatbaar is.

17 Verzoekende partij in de vierde zaak laakt voorts dat deze verplichting tot algemene en ongedifferentieerde bewaring de criminaliteit in het algemeen bestrijdt, terwijl een dergelijke bewaring slechts is toegelaten in het kader van de strijd tegen zware criminaliteit (die enkel inbreuken op de in artikel 5 en 8 van het Handvest gewaarborgde grondrechten kan rechtvaardigen, hetgeen volstrekt niet het geval is wanneer het gaat om fraude of kwaadwillig gebruik van het netwerk) en in elk geval onevenredig is. De opgenomen bewaarplicht zou dus duidelijk niet vallen onder de in artikel 15, lid 1, van richtlijn 2002/58/EG bedoelde uitzondering.

18 Zij beroept zich op de artikelen 11, 12, 22 en 29 van de Grondwet, gelezen al dan niet in samenhang met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, artikel 8 EVRM, de artikelen 5, 6 en 15 van richtlijn 2002/58/EG en de artikelen 13 en 54 van richtlijn (EU) 2016/680.

19 Voorts meent zij dat artikel 5, punt 5, van de bestreden wet voorziet in een te lange bewaartermijn.

20 Subsidiair verzoekt zij om een prejudiciële vraag aan het Hof te stellen om te bepalen of artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in samenhang met de artikelen 7, 8 en 52, lid 1, van het Handvest, in de weg staat aan een algemene verplichting voor de operatoren en de aanbieders van elektronischecommunicatiediensten, die van toepassing is op andere feiten dan ernstige strafbare feiten, om, ten behoeve van de opsporing en de analyse van een vermeende fraude of een vermeend kwaadwillig gebruik van een elektronischcommunicatienetwerk, de verkeers- en locatiegegevens in de zin van die richtlijn, die gegenereerd of verwerkt worden in het kader van de levering van die diensten, te bewaren.

21 Verzoekende partijen in de vijfde zaak bekritiseren eveneens het algemene en ongedifferentieerde karakter van de bewaring die in strijd is met artikel 6 van

richtlijn 2002/58/EG, op grond waarvan verkeersgegevens moeten worden gewist of anoniem gemaakt, zodra zij niet langer nodig zijn (hetgeen niet is voorzien) en ook niet voldoet aan de uitzondering, zoals bedoeld in artikel 15, lid 1 van deze richtlijn, aangezien het niet om ernstige strafbare feiten of een vraagstuk van nationale veiligheid gaat.

22 Zij richten zich in wezen op de bepalingen die in punt 20 van deze samenvatting worden genoemd, waarbij zij hieraan nog toevoegen artikel 15 van de Grondwet (onschendbaarheid van de woning), artikel 4 van het Verdrag betreffende de Europese Unie (hierna: „VEU”) en de AVG.

23 De Ministerraad merkt op dat artikel 5 van de bestreden wet tot doel heeft fraude en kwaadwillig gebruik van netwerken te bestrijden alsook de veiligheid en de goede werking van netwerken mogelijk te maken. Daartoe verplicht het met name om bepaalde metagegevens die *noodzakelijk* worden geacht, te bewaren, hetgeen veronderstelt dat de operatoren bij elk geval van bewaring de daarbij betrokken belangen tegen elkaar afwegen.

24 Bij de bestrijding van fraude en kwaadwillig gebruik van netwerken zijn de operatoren immers het beste in staat om de noodzaak van het bewaren van metagegevens in het kader van de door de wetgever vastgelegde doeleinden, concreet te beoordelen.

25 Dat die maatregel noodzakelijk moet zijn is overigens zorgvuldig onderbouwd in de parlementaire voorbereiding (Parl. St., Kamer 2021-2022, DOC 55-2572). Er is voorts voorzien in een noodzakelijkheidstoets voordat de operatoren overgaan tot bewaring.

26 De databanken komen op geautomatiseerde wijze tot stand, waardoor een individueel geval pas in aanmerking kan worden genomen wanneer er toegang bestaat tot een bewaard gegeven.

27 De Ministerraad voert aan dat de periode van twaalf maanden gedurende welke de gegevens moeten worden bewaard, is onderbouwd in de parlementaire voorbereiding en aan die algemene termijn kan worden gesleuteld om deze te laten aansluiten bij de technische realiteit waarmee de operatoren worden geconfronteerd. De wetgever heeft er daarom voor gezorgd dat er termijnen worden vastgesteld die beantwoorden aan de doeleinden die hij wil nastreven.

28 Uit het feit dat de bestreden wet meerdere termijnen onderscheidt, blijkt dat de wetgever de bewaarplicht, met inbegrip van de duur ervan, tot het strikt noodzakelijke heeft willen beperken.

29 De bestrijding van fraude en kwaadwillig gebruik van netwerken alsook de veiligheid en een goede werking van netwerken, worden als doeleinden niet uitgesloten door de rechtspraak van het Hof, die zich niet over die onderwerpen heeft uitgesproken.

30 De bewaarde gegevens zijn overigens onvoldoende om het doel van identificatie te verwezenlijken, aangezien de inlichtingen over de burgerlijke identiteit met elkaar moeten worden vergeleken om de betrouwbaarheid ervan te waarborgen.

31 Daarnaast worden bepaalde gegevens bedoeld in artikel 5 van de bestreden wet hoe dan ook reeds door de operatoren gebruikt om incidenten of anomalieën op te sporen en om verkeersstromen op hun netwerken te beheren en te optimaliseren.

32 Tot slot vormen artikel 15, lid 1, van de richtlijn 2002/58/EG en artikel 23 van de AVG volgens de Ministerraad een geldige rechtsgrond voor artikel 5 van de bestreden wet, die de door deze bepalingen toegestane grenzen aangeeft, zoals in de parlementaire voorbereiding van die wet wordt onderstreept. Bij twijfel daarover zou het Hof kunnen worden geadieerd.

*Analyse van het Grondwettelijk Hof*

33 Het Grondwettelijk Hof merkt op dat artikel 22 van de Grondwet, gelezen in samenhang met artikel 8 EVRM en de artikelen 7 en 8 van het Handvest (artikelen die soortgelijke grondrechten waarborgen) en artikel 52 van dit Handvest, de verplichting oplegt dat de inmenging in het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens in duidelijke en voldoende nauwkeurige bewoordingen wordt geformuleerd die het mogelijk maken de hypothesen te voorzien waarin de wetgever een dergelijke inmenging toestaat.

34 Inzake de bescherming van de persoonsgegevens impliceert dat vereiste van voorzienbaarheid dat voldoende precies moet worden bepaald in welke omstandigheden persoonsgegevens mogen worden verwerkt (EHRM, 4 mei 2000, Rotaru t. Roemenië, ECLI:CE:ECHR:2000:0504JUD002834195, § 57 en 4 december 2008, S. en Marper t. Verenigd Koninkrijk, ECLI:CE:ECHR:2008:1204JUD003056204, § 99).

35 Het vereiste dat de beperking bij wet dient te worden ingesteld, houdt met name in dat de rechtsgrond die de inmenging in die rechten toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen (HvJ, 6 oktober 2020, C-623/17, Privacy International, ECLI:EU:C:2020:790, punt 65).

36 Derhalve moet eenieder een voldoende duidelijk beeld kunnen hebben van de verwerkte gegevens, de bij een bepaalde gegevensverwerking betrokken personen, alsmede de voorwaarden voor en de doeleinden van de verwerking.

37 Uit de parlementaire voorbereiding van de bestreden wet blijkt dat artikel 5, punten 4 en 5, van deze wet met name beoogt artikel 15 van richtlijn 2002/58/EG om te zetten, voor zover dit artikel 15 afwijkt van artikel 6, lid 5, van die richtlijn en de lidstaten toelaat maatregelen te nemen om ervoor te zorgen dat onbevoegd gebruik van het elektronischecommunicatiesysteem wordt voorkomen, onderzocht, opgespoord en vervolgd.

38 Die doelstellingen zijn legitiem in de zin van artikel 8 van het EVRM en artikel 52 van het Handvest.

39 In dat kader heeft de wetgever gepreciseerd dat het niet mogelijk was om te voorzien in een bewaring van gegevens „die reactief en doelgericht is van[af] het begin" wegens de structuur zelf van de betrokken netwerken en diensten. Hij was bovendien van oordeel dat het in artikel 5, punten 4 en 5, van de bestreden wet bepaalde systeem voor de bewaring van verkeersgegevens bestaat „in het belang van de eindgebruikers van de diensten van de operator" en ertoe strekt dat de slachtoffers van fraude of kwaadwillig gebruik van het netwerk de dader ervan kunnen identificeren.

40 Dat systeem wordt overigens voorgesteld als „[houdende] intrinsiek verband [...] met de verstrekking van de elektronischecommunicatiedienst" en als een manier om de wet van 13 juni 2005 te updaten, rekening houdend met het toenemende belang van de doelstelling van bestrijding van fraude en kwaadwillig gebruik van het netwerk in het Unierecht.

41 Het staat aan het Grondwettelijke Hof om na te gaan of de inmenging die artikel 5, punten 4 en 5, van de bestreden wet in het recht op eerbiediging van het privéleven en het recht op bescherming van de persoonsgegevens met zich meebrengt, geen onevenredige gevolgen heeft voor de personen waarop de in die bepaling beoogde maatregelen betrekking hebben.

42 Artikel 5, punt 4 van de bestreden wet voorziet, ten laste van de operatoren, in een verplichting tot bewaring van verschillende verkeersgegevens om „de gepaste maatregelen bedoeld in artikel 121/8, § 1, te [...] 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", voor zover de operatoren die gegevens verwerken „in het kader van de verstrekking van dat netwerk of die dienst".

43 De beoogde verkeersgegevens zijn „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" en „de locatie van de eindapparatuur van de communicerende partijen bij de aanvang en bij het einde van de communicatie" (artikel 122, paragraaf 4, eerste alinea, punt 1, van de wet van13 juni 2005 ingevoegd door artikel 5, punt 4, van de bestreden wet).

44 Ook wordt erin voorzien dat de operatoren verschillende verkeersgegevens betreffende de binnenkomende communicatie bewaren om de persoon die de communicatie doet te identificeren, namelijk „het telefoonnummer aan de bron van de binnenkomende communicatie", „het IP-adres dat werd gebruikt om de binnenkomende communicatie te versturen, het tijdstempel en de gebruikte poort", alsook „de precieze datums en tijdstippen van begin en einde van de binnenkomende communicatie" (eerste alinea, punt 2).

45 Krachtens artikel 122, § 4, eerste alinea, punt 5, van de wet van 13 juni 2005, verwerken de operatoren de verschillende beoogde gegevens voor de voormelde doeleinden.

46 De in artikel 122, § 4, eerste alinea, van de wet van 13 juni 2005 opgenomen lijst met verkeersgegevens is niet exhaustief.

47 Ten eerste wordt in artikel 122, § 4, tweede alinea, van deze wet vermeld dat „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, [...] de operator andere gegevens dan die bedoeld in de eerste alinea die voor deze doeleinden noodzakelijk worden geacht, [mag] bewaren en verwerken."

48 Die mogelijkheid voor de operatoren om andere gegevens dan die welke bij artikel 122, § 4, eerste alinea, zijn bepaald, te bewaren en te verwerken, is niet onderworpen aan een voorafgaand advies van of een melding aan het BIPT en de Gegevensbeschermingsautoriteit. In de parlementaire voorbereiding van de bestreden bepaling wordt die mogelijkheid niet onderbouwd.

49 Vervolgens voorziet artikel 122, § 4, derde alinea, van de wet van 13 juni 2005 erin dat „de Koning [...], bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het [BIPT] en van de Gegevensbeschermingsautoriteit, de verkeersgegevens waarvan de bewaring als noodzakelijk moet worden beschouwd voor het nastreven van de in deze paragraaf bedoelde doeleinden, [kan] preciseren en uitbreiden".

50 De parlementaire voorbereiding van deze bepaling motiveert die machtiging met het feit dat fraude mettertijd aanzienlijk evolueert en dat de bewaarde gegevens kunnen verschillen afhankelijk van de verstrekte elektronischecommunicatiedienst, de omvang van de operator, de tools waarover die beschikt en de gebruikers van de dienst.

51 De in artikel 122, § 4, eerste alinea, punt 1, van de wet van 13 juni 2005 beoogde verkeersgegevens worden in principe gedurende vier maanden bewaard. De in punt 2 van dit artikel beoogde gegevens worden in principe gedurende twaalf maanden bewaard.

52 Deze termijnen kunnen worden verlengd. Punt 3 van artikel 122, § 4, eerste alinea, van de wet van 13 juni 2005 bepaalt dat „de in eerste alinea beoogde gegevens die betrekking hebben op een specifieke fraude of een specifiek kwaadwillig gebruik van een netwerk" worden bewaard „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 punt 1", terwijl punt 4 van dit artikel, preciseert dat de in punt 2 beoogde gegevens die betrekking hebben op een specifiek kwaadwillig gebruik van het netwerk worden bewaard „gedurende de periode die nodig is voor de verwerking van dit kwaadwillig gebruik, in voorkomend geval langer dan een termijn van twaalf maanden bedoeld in punt 2".

53 Artikel 122, § 4/1, van de wet van 13 juni 2005 voorziet op zijn beurt in de mogelijkheid voor de operatoren om de verkeersgegevens „die nodig zijn om de veiligheid en correcte werking van hun elektronischecommunicatienetwerken en -diensten te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, daaronder begrepen om de oorsprong van die aanslag te identificeren", te bewaren en te verwerken.

54 Die mogelijkheid voor de operatoren is ook niet onderworpen aan een voorafgaand advies van of een melding aan het BIPT en de Gegevensbeschermingsautoriteit.

55 De verkeersgegevens waarvan sprake in artikel 122, § 4/1, eerste alinea, van de wet van 13 juni 2005 kunnen voor een duur van in principe twaalf maanden worden bewaard. De gegevens met betrekking tot een „specifieke" schending van de veiligheid van het netwerk kunnen echter worden bewaard „gedurende de periode die nodig is om deze te verwerken, in voorkomend geval langer dan de termijn van twaalf maanden bedoeld in de tweede alinea" (artikel 122, § 4/1, derde alinea).

56 Artikel 122, § 4, van de wet van 13 juni 2005 voorziet, enerzijds, in een algemene en systematische bewaring van de in dit artikel bedoelde verkeersgegevens en legt, anderzijds, een verplichting tot bewaring en verwerking op aan de operatoren, maar laat hen bepalen welke gegevens van de gegevens bedoeld in artikel 122, § 4, eerste alinea, punten 1 en 2, moeten worden bewaard.

57 Met andere woorden, in het kader van deze bepaling vormt de verplichting tot bewaring van de gegevens niet de uitzondering maar de regel.

58 Deze conclusie geldt des te meer daar krachtens artikel 122, § 4, vierde alinea, van de wet van 13 juni 2005, de door de operatoren bewaarde verkeersgegevens die verband houden met vermeende fraude of vermeend kwaadwillig gebruik, aan de bevoegde autoriteiten kunnen worden doorgestuurd, met name aan de gerechtelijke autoriteiten, de politiediensten en de officieren van gerechtelijke politie van het BIPT, zodat de bewaring en de verwerking van gegevens door de operatoren op basis van artikel 122, § 4, van de wet van 13 juni 2005 aanleiding kunnen geven tot strafrechtelijke vervolging.

59 Wat betreft artikel 122, § 4/1, van deze wet, dient te worden opgemerkt dat deze bepaling niet preciseert welke gegevens kunnen worden bewaard.

60 Daarenboven kunnen de gegevens met betrekking tot een „specifieke" schending van de veiligheid van het netwerk „langer dan de termijn van twaalf maanden bedoeld in de tweede alinea" worden bewaard, zonder dat in de tekst van artikel 122, § 4/1, van deze wet, noch in de parlementaire voorbereiding van de bestreden wet, wordt gepreciseerd wat de hypothese van een specifieke schending omvat.

61 Op de datum van de uitspraak van dit arrest heeft het Hof zich nog niet hoeven uitspreken over de uitlegging van artikel 15 van de richtlijn 2002/58/EG voor zover het de lidstaten toestaat maatregelen te nemen tot bewaring van gegevens uit elektronische communicatie om ervoor te zorgen dat onbevoegd gebruik van het elektronischecommunicatiesysteem wordt voorkomen, onderzocht, opgespoord en vervolgd.

62 [Verzoekende] partijen verschillen van mening over de uitlegging die moet worden gegeven aan artikel 15 van de richtlijn 2002/58/EG, voor zover het betrekking heeft op het voormelde doel en voor zover het al dan niet in dat kader in die zin moet worden uitgelegd dat het toestaat nationale maatregelen te nemen zoals die welke zijn bedoeld in artikel 5, punten 4 en 5, van de bestreden wet.

63 Aangezien deze zaak twijfel doet rijzen over de uitlegging van artikel 15 van richtlijn 2002/58/EG, moet het Hof een eerste prejudiciële vraag worden gesteld.

***Bewaring van locatiegegevens (artikel 6 van de bestreden wet)***

64 In artikel 6, punt 1, van de bestreden wet wordt artikel 123 van de wet van 13 juni 2005 als volgt gewijzigd:

„1° paragraaf 1 wordt vervangen als volgt:

Artikel 123, § 1. Onverminderd de toepassing van de AVG en van de wet van 30 juli 2018 [betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens] 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 een specifieke fraude of een 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.”

*Standpunt van partijen*

65 Verzoekende partijen in de derde zaak beroepen zich op schending van de artikelen 11, 12, 22 en 29 van de Grondwet, artikel 15, lid 1, en de artikelen 5, 6 en 9 van richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, de artikelen 6, 8, 10, 11 en 18 van het EVRM en de artikelen 13 en 54 van richtlijn (EU) 2016/680, voor zover artikel 6 van de bestreden wet een algemene verplichting tot bewaring van de communicatiegegevens invoert, zonder dat die bewaring noodzakelijk, noch strikt beperkt ten aanzien van het nagestreefde doel blijkt te zijn.

66 Verzoekende partijen in de vijfde zaak beroepen zich op schending van de artikelen 10, 11, 13, 15, 22, 23 en 29 van de Grondwet, gelezen al dan niet in samenhang met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 EVRM, de artikelen 7, 8, 11, 47 en 52 van het Handvest, artikel 5, lid 4, VEU, alsook artikel 6 van de richtlijn 2002/58/EG, met richtlijn (EU) 2016/680 en met de AVG, voor zover artikel 6 van de bestreden wet toestaat om de hierin beoogde gegevens gedurende twaalf maanden te bewaren om de goede werking en de veiligheid van het netwerk te waarborgen, terwijl artikel 9 van richtlijn 2002/58/EG een dergelijke verwerking uitsluit.

67 Anderzijds beroepen zij zich op schending van de artikelen 10, 11, 15, 22 en 29 van de Grondwet, gelezen al dan niet in samenhang met de in het vorige punt genoemde artikelen van het EVRM, het Handvest, en het VEU, alsook met richtlijn 2002/58/EG, richtlijn (EU) 2016/680 en de AVG, voor zover artikel 6 van de bestreden wet een verplichting tot algemene en ongedifferentieerde bewaring van de gegevens creëert ten gunste van de operatoren die in het kader van hun opdrachten handelen, hetgeen te vaag en te ruim is.

68 De Ministerraad brengt ten aanzien van de locatiegegevens geen argumentatie naar voren die verschilt van die betreffende de bewaring van verkeersgegevens die gebaseerd is op de de bestrijding van fraude en kwaadwillig gebruik van netwerken, en de veiligheid en de goede werking van de netwerken, als doelstellingen.

*Analyse van het Grondwettelijk Hof*

69 Het Grondwettelijk Hof merkt op dat bovengenoemde verzoeksters zich in wezen beroepen op schending van het recht op eerbiediging van het privéleven en van het recht op bescherming van persoonsgegevens en dat de betrokken bepaling van de bestreden wet beoogt artikel 9 van richtlijn 2002/58/EG om te zetten.

70 Voor zover de betrokken bepaling voorziet in de bewaring van de andere locatiegegevens dan verkeersgegevens die betrekking hebben op een abonnee of

een eindgebruiker wanneer de gegevens anoniem zijn gemaakt (3°) en wanneer de verwerking past in het kader van de levering van een dienst die gebruik maakt van verkeersgegevens of locatiegegevens (4°) – op voorwaarde dat, in dat laatste geval, de abonnee of de eindgebruiker krachtens artikel 123, § 2, vooraf zijn toestemming heeft gegeven –, past die bepaling in de door artikel 9, lid 1, van deze richtlijn beoogde gevallen.

71 De betrokken bepaling heeft daarentegen ook betrekking op andere hypotheses van bewaring van gegevens, dan die welke zijn toegelaten in dit artikel.

72 Wat die andere hypotheses betreft, dient te worden verwezen naar artikel 15, lid 1, van deze richtlijn, dat toestaat de reikwijdte van de met name in artikel 9 ervan bepaalde rechten te beperken, „indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale [veiligheid], 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 elektronischecommunicatiesysteem”.

73 De grieven van de verzoekende partijen hebben meer in het bijzonder betrekking op die andere hypotheses (als bedoeld in artikel 123, § 1, 1°, 2° en 5°, van de wet van 13 juni 2005, zoals gewijzigd bij artikel 6, punt 1, van de bestreden wet).

74 De in artikel 123, § 1, 1° en 2°, van de wet van 13 juni 2005 bedoelde hypotheses maken het mogelijk om onbevoegd gebruik van het elektronische-communicatiesysteem in de zin van artikel 15, lid 1, van richtlijn 2002/58/EG te voorkomen, te onderzoeken, op te sporen en te vervolgen.

75 Het staat aan het Grondwettelijk Hof om na te gaan of de inmenging die deze bepalingen in het recht op eerbiediging van het privéleven en het recht op bescherming van de persoonsgegevens veroorzaken, in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter voorkoming van onbevoegd gebruik van het elektronischecommunicatiesysteem.

76 Op grond van deze bepalingen bepalen de operatoren welke andere locatiegegevens dan de verkeersgegevens kunnen worden bewaard en verwerkt. Zij beoordelen ook in elk concreet geval de noodzaak van die bewaring en die verwerking.

77 Bovendien kunnen de voorziene bewaringstermijnen van twaalf maanden (noodzakelijk voor de goede werking en de veiligheid van het netwerk of de dienst) en van vier maanden (noodzakelijk om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren), worden verlengd respectievelijk „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” en „in geval van een specifieke fraude of een specifiek kwaadwillig gebruik waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode”.

78 Om de redenen als die zijn vermeld in de punten 59 tot en met 61 van deze samenvatting, is er naar het oordeel van het Hof op dit punt zodanige twijfel over de uitlegging van artikel 15, lid 1, van richtlijn 2002/58/EG dat het Hof een tweede prejudiciële vraag moet worden gesteld.

***Bevoegdheden van de officieren van gerechtelijke politie van het BIPT (artikel 24 van de bestreden wet)***

79 Artikel 24 van de bestreden wet voegt in de wet van 17 januari 2003 „met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector” (hierna: wet van 17 januari 2003) een artikel 25/1 in, dat bepaalt:

„§ 1. Om een inbreuk bedoeld in artikel 145, § 3 of § 3bis, van de wet van 13 juni 2005 betreffende de elektronische communicatie [respectievelijk de uitvoering van elektronische communicatie ter verkrijging van een ongeoorloofd voordeel en gebruik van elektronische communicatie teneinde iemands contactpersoon lastig te vallen] of in artikel 24, § 1, 2° [overtredingen van het Strafwetboek gepleegd met apparatuur, netwerken of diensten van elektronische communicatie of radiocommunicatie], te kunnen opsporen, vaststellen of vervolgen, kan een officier van gerechtelijke politie van het [BIPT], schriftelijk:

1° van een operator eisen om te antwoorden op een verzoek om identificatiegegevens, dat voor deze doeleinden noodzakelijk is;

2° de medewerking vorderen van [financiële instellingen] op basis van het kenmerk van de onlinebetaling specifiek voor een elektronischecommunicatiedienst die voorafgaandelijk meegedeeld is door een operator overeenkomstig de bepaling onder 1°, om de persoon te identificeren die de dienst heeft betaald;

3° de medewerking vorderen van de gesloten centra of woonunits [...] waar de inschrijving van de abonnee op een elektronischecommunicatiedienst heeft plaatsgevonden, op basis van de contactgegevens van het centrum of de woonunit die voorafgaandelijk meegedeeld zijn door een operator overeenkomstig de bepaling onder 1°, om de abonnee te identificeren;

4° de medewerking vorderen van alle andere rechtspersonen die abonnee zijn van een operator, of die intekenen in naam en voor rekening van natuurlijke personen op een elektronischecommunicatiedienst, op basis van de gegevens die voorafgaandelijk meegedeeld zijn door een operator overeenkomstig de bepaling onder 1°, om de abonnee of de gewoonlijke gebruiker van de dienst te identificeren.

[...]

§ 2. Ten behoeve van de vervulling van zijn opdrachten kan een officier van gerechtelijke politie van het [BIPT] schriftelijk eisen om te antwoorden op een

verzoek om metagegevens, die nodig zijn om een inbreuk bedoeld in artikel 145, § 3, of § 3bis, van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 24, § 1, 2°, te kunnen opsporen, vaststellen of vervolgen.

Tenzij in geval van een naar behoren gerechtvaardigde hoogdringendheid, mag de officier van gerechtelijke politie van het [BIPT] het verzoek aan de operator pas richten na het voorleggen van een schriftelijk en met redenen omkleed verzoek aan de onderzoeksrechter en na schriftelijke toestemming van deze laatste.

In geval van een naar behoren gerechtvaardigde hoogdringendheid zoals bedoeld in het tweede lid, deelt de officier van gerechtelijke politie van het [BIPT] na de verzending van het verzoek naar de operator onverwijld een kopie van dit verzoek, de motivering van het verzoek alsook de rechtvaardiging van de hoogdringendheid mee aan de onderzoeksrechter. De onderzoeksrechter voert daarna een controle uit.

Wanneer na deze latere controle de onderzoeksrechter weigert de geldigheid te bevestigen van het verzoek dat door de officier van gerechtelijke politie van het [BIPT] naar de operator is verstuurd, laat deze officier dat onverwijld aan de betrokken operator weten en wist hij de ontvangen metagegevens.

[...]”.

*Standpunt van partijen*

80 Volgens verzoekende partij in de vierde zaak schendt artikel 25/1 van de wet van 17 januari 2003 de artikelen 11, 12, 22 en 29 van de Grondwet, gelezen al dan niet in samenhang met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, artikel 8 EVRM, de artikelen 5, 6 en 15 van richtlijn 2002/58/EG en de artikelen 13 et 54 van richtlijn (EU) 2016/680, voor zover het in het kader van een strafrechtelijke procedure toegang tot bepaalde gegevens toestaat, via een officier van gerechtelijke politie, die geen onafhankelijke instantie is, en voor zover het geen rechterlijke toetsing voorafgaande aan die toegang oplegt.

81 Zij laakt eveneens het feit dat de persoon tot wiens gegevens toegang wordt verschaft, niet wordt geïnformeerd, alsook het feit dat er geen rechtsmiddelen zijn in geval van een onrechtmatige toegang tot de gegevens.

82 Subsidiair verzoekt zij om het Hof een prejudiciële vraag te stellen over het niet-informeren van de betrokken persoon.

83 Zonder zich tegen het stellen van deze vraag te verzetten, stelt de Ministerraad dat deze vraag niet nuttig is voor de oplossing van het geschil, aangezien artikel 37 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens in het algemeen voorziet in een recht op informatie.

*Analyse van het Grondwettelijk Hof*

84 Artikel 25/1 van de wet van 17 januari 2003 staat een officier van gerechtelijke politie van het [BIPT] toe toegang te verkrijgen tot de gegevens in twee gevallen. Ten eerste kan de officier van gerechtelijke politie toegang verkrijgen tot identificatiegegevens om de in artikel 145, §§ 3 en 3bis, van de wet van 13 juni 2005 en in artikel 24, § 1, 2°, van de wet van 17 januari 2003 bedoelde inbreuken op te sporen, vast te stellen of te vervolgen (artikel 25/1, § 1). Ten tweede kan de officier van gerechtelijke politie, ten behoeve van de vervulling van zijn opdrachten, toegang verkrijgen tot de metagegevens die nodig zijn om deze inbreuken op te sporen, vast te stellen of te vervolgen (artikel 25/1, § 2).

85 Aangezien de bestreden bepaling verwijst naar bepalingen waaromtrent het Grondwettelijk Hof prejudiciële vragen heeft gesteld aan het Hof, wordt de behandeling van de grieven aangehouden in afwachting van het antwoord van het Hof op deze prejudiciële vragen.

**Prejudiciële vragen**

1. Dient 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), gelezen in samenhang met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden uitgelegd:

a) dat het zich verzet tegen een nationale wetgeving die voorziet in een verplichting voor de operatoren van elektronischecommunicatiediensten om in het kader van de verstrekking van dat netwerk of die dienst, de in die wetgeving bepaalde verkeersgegevens te bewaren en te verwerken gedurende een periode van, naargelang van het geval, vier of twaalf maanden, teneinde de gepaste, evenredige, preventieve en curatieve maatregelen te kunnen treffen om fraude en kwaadwillig gebruik op hun netwerken te voorkomen en te vermijden dat de eindgebruikers schade lijden of lastiggevallen worden, alsmede 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;

b) dat het zich verzet tegen een nationale wetgeving die deze operatoren toestaat om de betrokken verkeersgegevens langer dan de voormelde termijnen te bewaren en te verwerken, in geval van 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 of gedurende de periode die nodig is voor de verwerking van dat kwaadwillig gebruik;

c) dat het zich verzet tegen een nationale wetgeving die deze operatoren toestaat, zonder te voorzien in de verplichting om een voorafgaand advies te vragen of een melding te doen aan een onafhankelijke autoriteit, andere gegevens

dan die welke in de wet zijn bepaald, te bewaren en te verwerken 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;

d) dat het zich verzet tegen een nationale wetgeving die deze operatoren toestaat, zonder te voorzien in de verplichting om een voorafgaand advies te vragen of een melding te doen aan een onafhankelijke autoriteit, voor een duur van twaalf maanden de verkeersgegevens te bewaren en te verwerken die zij nodig achten om de veiligheid en de correcte werking van hun elektronischecommunicatienetwerken 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 en, in geval van een specifieke schending van de veiligheid van het netwerk, voor de duur die nodig is om deze te behandelen?

2. Dient artikel 15, lid 1, van richtlijn 2002/58/EG, gelezen in samenhang met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden uitgelegd:

a) dat het zich verzet tegen een nationale wetgeving die de operatoren van mobiele netwerken toestaat om in het kader van de verstrekking van dat netwerk of die dienst locatiegegevens, zonder dat de wetgeving precies omschrijft welke gegevens zijn bedoeld, te bewaren en te verwerken gedurende een periode van, naargelang van het geval, vier of twaalf maanden, wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of de dienst, of om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren;

b) dat het zich verzet tegen een nationale wetgeving die aan deze operatoren de mogelijkheid biedt om de locatiegegevens langer dan de voormelde termijnen te bewaren en te verwerken in geval van een specifieke schending van de veiligheid, een specifieke fraude of een specifiek kwaadwillig gebruik?

3. Indien het Grondwettelijk Hof op basis van de op de eerste of de tweede prejudiciële vraag verstrekte antwoorden tot de slotsom zou komen dat sommige bepalingen 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” een of meer van de verplichtingen niet nakomen die voortvloeien uit de in die vragen vermelde bepalingen, kan het dan de gevolgen van de voormelde bepalingen van de wet van 20 juli 2022 tijdelijk handhaven teneinde rechtsonzekerheid te voorkomen en mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen worden gebruikt voor de door de wet beoogde doeleinden?