UHASSELT
KNOWLEDGE IN ACTION

KU LEUVEN

Maastricht University

Faculteit Rechten

master in de rechten

Masterthesis

Dataretentie in het digitale tijdperk: een analyse van de nieuwe Belgische dataretentiewet in het licht van het Unierechtelijk kader

Sharleen Quarem

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting overheid en recht

PROMOTOR :

Prof. dr. Stijn SMET

2022
2023

De transnationale Universiteit Limburg is een uniek samenwerkingsverband van twee universiteiten in twee landen: de Universiteit Hasselt en Maastricht University.

UHASSELT
KNOWLEDGE IN ACTION

www.uhasselt.be
Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

UHASSELT
KNOWLEDGE IN ACTION

KU LEUVEN

Maastricht University

Faculteit Rechten

master in de rechten

Masterthesis

Dataretentie in het digitale tijdperk: een analyse van de nieuwe Belgische dataretentiewet in het licht van het Unierechtelijk kader

Sharleen Quarem

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting overheid en recht

PROMOTOR :

Prof. dr. Stijn SMET

Samenvatting

Het opzet van deze masterscriptie is een normatieve en evaluatieve analyse van de nieuwe Belgische dataretentiewet van 2022 in het licht van het Unierechtelijk kader. Het antwoord op de onderzoeksvraag moet duidelijk maken in welke mate de Belgische dataretentiewet van 2022 voldoet aan het Unierechtelijke kader en in welke mate uit deze analyse een noodzaak voortvloeit om dit kader te optimaliseren.

In het eerste onderdeel van deze thesis wordt dataretentie gekaderd binnen het ruimer debat van veiligheid-versus-vrijheid. Binnen dit hoofdstuk wordt de maatschappelijke context toegelicht, de concepten vrijheid en veiligheid verder uitgediept en vervolgens de meest belangrijke elementen van dit debat besproken. Het gaat met name over het niets-te-verbergen-argument, het alles-of-niets-argument, de kritische benadering van het veiligheidscriterium en de maatschappelijke waarde van privacy.

In het tweede onderdeel van de thesis wordt aan de hand van het wetgevend kader op het niveau van de Europese Unie en de rechtspraak van het Hof van Justitie de voornaamste criteria geïdentificeerd. Binnen het wetgevend kader wordt er aandacht geschonken aan het EU-Handvest en aan secundaire wetgeving, zoals de Algemene Verordening Gegevensbescherming en de E-Privacy Richtlijn. De criteria uit de rechtspraak van het hof van Justitie zijn gebaseerd op de volgende zeven arresten: (I) Tele2 Watson, (II) Ministerio Fiscal, (III) La Quadrature du net, (IV) Privacy International, (V) Prokuratuur , (VI) Commissioner of An Garda Síochána en (VII) SpaceNet en VD

In het derde onderdeel van deze thesis wordt de conformiteit van de nieuwe Belgische Dataretentiewet van 2022 met het Unierechtelijk kader geëvalueerd. Uit de analyse van de dataretentiewet van 2022 wordt duidelijk dat de Belgische wetgever de Europese criteria zoveel mogelijk heeft proberen omzetten, maar er niet altijd in is geslaagd om dit op een adequate manier te doen. Dit komt tot uiting in de bepaling over de versleuteling van gegevens, het gebrek aan duidelijke en nauwkeurige regels over de reikwijdte van algemene en ongedifferentieerde verzameling van verkeers- en locatiegegevens vastgelegd in art. 126/3, §2 tweede lid WEC en het feit dat er geen effectieve toetsing is ingevoerd hetzij door een rechtbank, hetzij door een onafhankelijke administratieve instantie waarvan de beslissing bindend is. Zo is ook de regeling van de gerichte bewaring in de telecomwet is op verschillende punten aan verbetering toe. Met betrekking tot de gerichte bewaring in het kader van een strafonderzoek, kan geconcludeerd worden dat de wetgever de criteria aangereikt door het Hof soepel heeft ingevuld en dat deze regeling ingaat tegen de ratio van de gerichte bewaring in real time. Ten slotte wat betreft de toegang tot de bewaarde gegevens, moet de invulling van zware criminaliteit en de kennnisgeving terug onder de loep genomen worden.

Uit deze analyse blijkt dat er een noodzaak bestaat om het kader op nationaal niveau de optimaliseren. Dezelfde conclusie kan gemaakt worden op het niveau van de Europese Unie, aangezien de meeste lidstaten moeilijkheden ondervinden om in overeenstemming te zijn met het Unierecht.

Dankwoord

Deze masterthesis werd geschreven met het oog op het behalen van de academische graad 'Master in de Rechten'. Het is het resultaat van vele nuttige uren in de rechtsbibliotheek, een uitstap naar het Coördinatieorgaan voor de dreigingsanalyse en talrijke schrijf- en herschrijfuren. Tot dit eindwerk zou ik echter niet geraakt zijn zonder de steun en raad van velen. Daarom zou ik graag enkele mensen willen bedanken.

Eerst en vooral wil ik mijn promotor, professor Smet, bedanken voor het naleeswerk, de nuttige feedback, het beantwoorden van vele vragen en de nodige flexibiliteit. Uw kritische en pertinente opmerkingen waren waardevol en leerrijk.

Daarnaast zou ik graag expliciet mijn vriend Lennert bedanken. Doorheen dit schrijfproces was hij de stem van de rede en gezond verstand. Bedankt om mij met beide voeten op de grond te houden wanneer de stress het overneemt, om mijn allergrootste supporter te zijn en om steeds het beste in mezelf naar boven te halen.

Bedankt Britt, voor jouw aanmoedigende woorden op de momenten dat ze nodig waren. Jouw vriendschap en positieve ingesteldheid zorgen voor licht wanneer het donker is.

Ten slotte bedank ik graag Alyssa, Jade en Yasmine, die al zeven jaren aan mijn zijde staan. Jullie onvoorwaardelijke steun en vriendschap liggen mij nauw aan het hart. Ik kan me geen betere vriendinnen wensen.

Inhoudsopgave

Lijst van afkortingen

EVRM	Europees Verdrag voor de Rechten van de Mens
EU-Handvest	Handvest van de grondrechten van de Europese Unie van 12 december 2007
EHRM	Europees Hof voor de Rechten van de Mens van de Raad van Europa
HvJ	Hof van Justitie
AVG	Algemene Verordening Gegevensbescherming
VSSE	Dienst voor de Veiligheid van de Staat
VEU	Verdrag betreffend de Europese Unie
Sw.	Strafwetboek
Sv.	Wetboek van Strafvordering
Dataretentierichtlijn	Richtl. Europees Parlement en de Raad nr. 2006/24, 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
Digital Rights Ireland	HvJ (Grote kamer) 8 april 2014, nrs. C-293/12 en C-594/12, ECLI:EU:C:2014:238, Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a. en Kärntner Landesregierung e.a.
Tele 2 Watson	HvJ (Grote kamer) 21 december 2016, nrs. C-203/15 en C-698/15, ECLI:EU:C:2016:970, Tele2 Sverige AB/Post-och telestyrelsen en Secretary of State for the Home Department/Tom Watson e.a.
Ministerio Fiscal	HvJ (Grote kamer) 2 oktober 2018, nr. C-207/16, ECLI:EU:C:2018:788, Ministerio Fiscal

La Quadrature du Net	HvJ (Grote kamer) 6 oktober 2020, nrs. C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, La Quadrature du Net e.a./Premier ministre e.a., French Data Network e.a. en Ordre des barreaux francophones et germanophone e.a./Conseils des ministres
Privacy International	HvJ (Grote kamer) 6 oktober 2020, nr. C-623/17, ECLI:EU:C:2020:790, Privacy International/Secretary of State for Foreign and Commonwealth Affairs e.a.
Prokuratuur	HvJ (Grote kamer) 2 maart 2021, nr. C-746/18, ECLI:EU:C:2021:152, H.K. Prokatuur
Commissioner of An Garda Siochána	HvJ (Grote kamer) 5 april 2022, nr. C-140/20, ECLI:EU:C:2022:258, Commissioner of An Garda Síochána
SpaceNet	HvJ (Grote kamer) 20 september 2022, nr. C-793/19 en C-794/19, ECLI:EU:C:2022:702, SpaceNet en Telekom Deutschland
VD	HvJ (Grote Kamer) 20 september 2022, nr. C-339/20, ECLI:EU:C:2022:703, VD
DRIPA	Data Retention and Investigatory Powers Act 2014 (GB) 17 juli 2014
Gw.	Grondwet
OCAD	Coördinatieorgaan voor de dreigingsanalyse
Privacycommissie	Commissie voor de bescherming van de persoonlijke levenssfeer
WEC	Wet 13 juni 2005 betreffende de elektronische communicatie

1. INLEIDING

1.1. Algemene toelichting

1. **DIGITALISERING –** Tegenwoordig leeft iedereen een digitaal leven. Elke keer dat het internet gebruikt wordt en berichten worden verzonden, iedere keer wanneer er wordt gebrowset, getikt, opgezocht en afgesloten worden er nieuwe gegevens gegenereerd over iemands communicatie- en surfgedrag. Iedereen laat als het ware een digitaal spoor na. Dit digitaal spoor wordt bewaard en verwerkt door elektronische communicatiediensten zoals bijvoorbeeld Messenger en WhatsApp. Hoewel de wezenlijke inhoud van de communicatie niet wordt bijgehouden, kan daarentegen wel de metadata van de communicatie worden bewaard. De term metadata verwijst in deze context naar informatie zoals iemands naam, met wie deze persoon contact heeft gehad, wanneer en hoelang dat contact was, evenals de webpagina's die werden opgezocht, hoelang deze werden bekeken en vanwaar de verbinding werd gemaakt. Zonder het goed te beseffen wordt er een volledig digitaal profiel gecreëerd en bewaard, eentje die veel informatie over iemands privéleven weergeeft.

2. **SPANNINGSVELD** – Dit digitaal profiel kan ingezet worden in de strijd tegen terrorisme en ernstige criminaliteit, de bescherming van de nationale veiligheid en de handhaving van de openbare orde. Hierbij kan er gedacht worden aan de drugsstrijd aan de Schelde[1], de aanslagen in Zaventem, overtuigende phishing-operaties en cybercriminaliteit[2]. Het bewaren van deze gegevens vormt een tool voor de rechtshandhavings- en veiligheidsdiensten om op een efficiënte wijze de punten te verbinden. Maar als deze bewaarde gegevens in de verkeerde handen vallen, kan dat gevaarlijke gevolgen teweegbrengen. Er ontstaan risico's zoals het onevenredig "in de gaten houden" van burgers, met inbegrip van politici en bedrijfsleiders. Zo kan bijvoorbeeld de locatie achterhaald worden van gezochte oppositieleiders of tegenhangers van het beleid in een autocratisch regime. Het bewaren van deze gegevens kan ook een "chilling effect" hebben op de vrijemeningsuiting, en dit in bijzonder voor verdedigers van de mensenrechten en minderheden. Het bewaren van deze gegevens, dat kan samengevat worden onder de term dataretentie, en de toegang tot deze gegevens vormen dan ook onderscheiden inmengingen in verschillende grondrechten. Daarbij zijn het recht op privacy en het recht op bescherming van persoonsgegevens in het bijzonder relevant. Elke bewaring van deze gegevens, toegang tot deze gegevens of het gebruik van deze gegevens is bijgevolg slechts mogelijk op basis van een wettelijke basis, voor een legitieme doelstelling en in zover dit gebruik in verhouding staat tot de doelstelling die werd nagestreefd.

3. **OVERZICHT –** Wetgevers en rechtscolleges in de Europese Unie worstelen al decennia met het zoeken naar een evenwicht tussen de bescherming van de grondrechten enerzijds en het

[1] J. VAN HORENBEEK, "'Met de wortel uitroeien': hoe de politiek de Antwerpse drugsbendes wil aanpakken", *De Morgen* 2023, www.demorgen.be/nieuws/met-de-wortel-uitroeien-hoe-de-politiek-de-antwerpse-drugsbendes-wil-aanpakken~b7dbac79/.
[2] N. VANHECKE, "Hacking treft Antwerpse stadsdiensten in hun kern", *De Standaard* 2022, www.standaard.be/cnt/dmf20221208_97860109.

garanderen van veiligheid anderzijds in het kader van dataretentie. In 2014 oordeelde het Hof van Justitie in de Digital Rights Ireland zaak dat een Europese dataretentierichtlijn die voorzag in een algemene bewaarplicht van communicatiegegevens in strijd was met het recht op de bescherming van persoonsgegevens. Dit markeerde het begin van de dataretentiesaga, die negen jaren later nog altijd in stand wordt gehouden door een heen en weer aan prejudiciële vragen tussen de hoogste nationale rechtscolleges en het Hof van Justitie. Het Hof van Justitie wordt namelijk verschillende malen opnieuw bevraagd over de verschillende aspecten van dataretentie en het evenwicht dat het heeft uitgewerkt. In België werd uiteindelijk op 8 augustus 2022 de derde dataretentiewet gepubliceerd die voorziet in nieuwe dataretentieregeling. Deze wet is de opvolger van twee vorige pogingen die werden vernietigd door het Grondwettelijk Hof. De nieuwe dataretentiewet van 2022 zou uiteindelijk dit evenwicht uitgewerkt door het Hof van Justitie moeten weerspiegelen.

4. **TOELICHTING –** In het licht van bovenstaande probleemstelling zal deze masterscriptie analyseren hoe dit evenwicht door het Hof van Justitie wordt ingevuld. Vervolgens wordt er nagegaan of de nieuwe Belgische dataretentiewet van 2022 voldoet aan de vooropgestelde Unierechtelijke vereisten. Ten slotte zal de vraag gesteld worden of dit uitgewerkt kader toe is aan optimalisatie. Om een antwoord te kunnen bieden op deze vragen, zal in hoofdstuk 2 het veiligheid-versus-vrijheid-debat verder toegelicht worden. Dit debat vormt namelijk het ruimer kader waarbinnen dataretentie zich situeert. Een notie van dit debat laat toe om de de doelstelling en proportionaliteitsvereiste op een juiste manier in te vullen. In hoofdstuk 3 volgt een analyse van het Europees wetgevend kader en het Europees jurisprudentieel kader. Het wetgevend kader is zowel gebaseerd op de relevante bepalingen van het primair unierecht, als op relevante secundaire wetgeving. Het jurispridentieel kader wordt aan de hand van zeven arresten uiteengezet en geanalyseerd, om zo de belangrijkste voorwaarden te filteren. In hoofdstuk 4 wordt ten slotte de nieuwe dataretentiewet van 2022 onder het vergrootglas gehouden. Aan de hand van de criteria die voortkomen uit hoofdstuk 3 worden de kernelementen van de dataretentiewet van 2022 getoetst op hun conformiteit. Uit deze analyse zal blijken of een optimalisatie van het kader noodzakelijk is.

1.2. Methodologie

1.2.1. Onderzoeksvraag

5. **HOOFDONDERZOEKSVRAAG –** Deze masterscriptie beoogt de volgende hoofdonderzoeksvraag te beantwoorden:

   "In welke mate voldoet de nieuwe Belgische dataretentiewet aan het Unierechtelijk kader en in welke mate vloeit uit de analyse een noodzaak voort om dit kader te optimaliseren?"

6. **SUBONDERZOEKSVRAGEN –** Deze hoofdonderzoeksvraag zal worden beantwoord aan de hand van de volgende subonderzoeksvragen, die de structuur van de masterscriptie weerspiegelen:
   - Subonderzoeksvraag 1: *"Binnen welk ruimer debat kadert dataretentie in de Europese Unie?"*
   - Subonderzoeksvraag 2: *"Hoe ziet het dataretentiekader eruit op het niveau van de Europese Unie?"*
   - Subonderzoeksvraag 3: *"Voldoet de nieuwe Belgische dataretentiewet aan het Unierechtelijk kader?"*
   - Subonderzoeksvraag 4: *"In welke mate vloeit uit de analyse een noodzaak voort om dit kader te optimaliseren?"*

1.2.2. Onderzoeksmethode

7. **HOOFDSTUK 2 –** Hoofdstuk 2 correspondeert met subonderzoeksvraag 1. De doelstelling van dit hoofdstuk is tweeledig, namelijk zowel het ruimer debat veiligheid-versus-vrijheid schetsen als de belangstelling voor dit ruimer debat benadrukken. Dataretentie brengt namelijk een inmenging teweeg in de rechten en vrijheden van burgers, wat vragen doet rijzen rond de doelstelling en proportionaliteit ervan. Dit hoofdstuk is noodzakelijk in het licht van de hoofdonderzoeksvraag omdat dataretentie niet los kan gezien worden van de rechtsfilosofische ontwikkelingen en de maatschappelijke impact die het heeft. Aangezien dataretentie een inmenging betekent in de rechten en vrijheden van burgers, is het belangrijk om de drogredenen te kunnen identificeren wanneer het gaat over de rechtvaardiging van de inperking binnen een democratische samenleving. Om de voorgeschreven doelstellingen te bereiken, werden de volgende vragen gesteld:
   - Binnen welke maatschappelijke context is dataretentie belangrijk geworden?
   - Wat is het belang van privacy en veiligheid in een democratische samenleving?
   - Wat houden de concepten privacy en veiligheid in?
   - Hoe wordt dit debat gevoerd en wat zijn de schijnargumenten aan beide kanten?
   - Hoe moet het debat gevoerd worden?

   Om deze vragen op te lossen werd er voor de maatschappelijke context en het belang van privacy en veiligheid in een democratische samenleving voornamelijk gebruik gemaakt van vier databanken: (I) Jurisquare, (II) Hein, (III) Google Scholar en (IV) Limo Libis.

Op basis van de zoektermen "data retention in society", "data retention and ethics" en "origins of data retention" voor de maatschappelijke context werd erop zoek gegaan naar rechtsleer die een inleiding gaven over het ontstaan van dataretentie in de Europese Unie. Op basis van zoektermen gelijkaardig aan "importance of data retention" werd evenzeer gezocht naar rechtsleer. Wat betreft de definiëring van de concepten privacy en veiligheid, werden de volgende databanken gebruikt: (I) Jurisquare, (II) Kluwer Navigator, (III) Limo Libis en (IV) Google Scholar. Aan de hand van de zoektermen "definition of" werden bijdragen gezocht die de concepten omschreven. Vervolgens werd de sneeuwbalmethode toegepast. Voor de definitie van de veiligheidsconcepten werd nog extra gekeken naar overheidssites, rapporten van de veiligheidsdiensten, het Strafwetboek en het Wetboek van Strafvordering.

De manier waarop het debat gevoerd wordt en de identificatie van de schijnargumenten steunt voornamelijk op twee grote werken als basis. Van hieruit werd gekeken welke relevante elementen aan bod kwamen voor het debat. Deze werden ingegeven in de databanken om een grondigere analyse te doen. Dezelfde werkwijze werd gehanteerd voor het identificeren van de schijnargumenten. Met betrekking tot de vraag hoe het debat moet gevoerd worden, werd er op basis van de voorgaande analyse een eigen mening gevormd.

8. **HOOFDSTUK 3 –** Hoofdstuk 3 komt overeen met subonderzoeksvraag 2. De doelstelling van dit hoofdstuk is om de verschillende bewaarplichten te identificeren op het niveau van de Europese Unie, samen met de doelstellingen die ze moeten nastreven en de voorwaarden waaraan ze moeten voldoen om gerechtvaardigd te zijn in een democratische samenleving. Dit hoofdstuk is noodzakelijk in het licht van de hoofdonderzoeksvraag omdat het de criteria weergeeft waaraan de nieuwe Belgische dataretentiewet van 2022 zal getoetst worden. Om de voorgeschreven doelstellingen te bereiken, werden de volgende vragen gesteld:
    - Welke bepalingen van het primair Unierecht zijn relevant?
    - Welke secundaire EU-wetgeving is van toepassing?
    - Wat zijn de belangrijke arresten van het Hof van Justitie?
    - Welke bewaarplichten kunnen geïdentificeerd worden in de rechtspraak van het Hof van Justitie?
    - Welke doelstellingen moeten de verschillende bewaarplichten nastreven?
    - Aan welke voorwaarden moeten deze bewaarplichten voldoen om gerechtvaardigd te zijn in een democratische samenleving?

Om tot een antwoord te komen op deze vragen werden de mijlpaalarresten opgezocht via Curia en een selectie gemaakt van de zeven belangrijkste cases. Deze selectie werd gebaseerd op verwijzingen door het Grondwettelijk Hof naar de rechtspraak van het Hof van Justitie en op rechtsleer. De bijdragen in de rechtsleer werden gevonden via Jurisquare met de zoekterm "dataretentie". Vervolgens werden de arresten grondig doorgelezen. De volgende stap was elk arrest apart ingeven in verschillende databanken zoals onder andere Jura, Jurisquare, Hein en Limo Libis om bijdragen te vinden die de analyse van het Hof en de uitkomst van het arrest beschreven. Op deze manier werden de voorwaarden gedistilleerd uit de rechtspraak en de rechtsleer.

Vormelijk werd ervoor gekozen om de analyse van de arresten op te delen in drie delen: (I) feiten, (II) analyse van het Hof en (III) conclusie. De tussenconclusies die bij elk arrest worden gegeven weerspiegelen de evolutie die het Hof van Justitie heeft gemaakt en vormen de basis voor het schematisch overzicht. Dit schematisch overzicht wordt ondergebracht onder de ondertitel "synthese', waar de tabel wordt geplaatst binnen de algemene rechtsleer.

9. **HOOFDSTUK 4** – Hoofdstuk 4 beantwoordt subonderzoeksvraag 3. Het doel van dit hoofdstuk bestaat erin om na te gaan of de Belgische nieuwe dataretentiewet van 2022 voldoet aan de criteria die voortkomen uit het Unierechtelijk kader. Dit hoofdstuk draagt rechtstreeks bij aan de oplossing van de hoofdonderzoeksvraag. Om de doelstelling van dit hoofdstuk te bereiken, werden de volgende vragen gesteld:
    - Wat is de voorgeschiedenis van de nieuwe Belgische dataretentiewet?
    - Wat zijn de belangrijkste elementen van de nieuwe Belgische dataretentiewet?
    - Aan welke voorwaarden moet elk van deze belangrijkste onderdelen van de nieuwe Belgische dataretentiewet voldoen om in overeenstemming te zijn met het Unierechtelijk kader?
    - Zijn deze elementen in overeenstemming met het Unierechtelijk kader?

    Om een antwoord te kunnen formuleren op deze vragen werd er voor de voorgeschiedenis van de nieuwe Belgische dataretentiewet een analyse gemaakt van voornamelijk drie soorten bronnen. Ten eerste gaat het over de memorie van toelichting bij elk van de drie dataretentiewetten die in België tot stand zijn gekomen. De tweede bron bestaat uit bijdragen in de rechtsleer die de evolutie van dataretentie in België weergeven, alsook het samenspel tussen het ontstaan van de wetten en de arresten van het Hof van Justitie en het Grondwettelijk Hof weerspiegelen. Ten derde vormen de arresten van het Grondwettelijk Hof inhoudelijk mee de basis voor de analyse. Om deze bronnen te identificeren, werden de memories van toelichting opgezocht op de website van de Kamer. Deze werden vervolgens inhoudelijk grondig doorgenomen. Om de bijlagen in de rechtsleer in kaart te brengen, werd er in de rechtsbibliotheek van Hasselt en op de online databanken Jura, Jurisquare en Limo Libis gezicht naar rechtsleerbijdragen met een gelijkaardige zoekterm aan "dataretentie in België". Ook werd er gezocht naar annotaties en bijdragen over de relevante arresten van het Grondwettelijk Hof.

    Met het oog op de belangrijkste elementen uit de nieuwe Belgische dataretentiewet te halen, werd er gekeken naar de bepalingen die waren vernietigd door het Grondwettelijk Hof en de knelpunten die in de arresten van het Hof van Justitie naar voren kwamen. Voor de volledigheid van de analyse werd het personeel en materieel toepassingsgebied mee opgenomen in de analyse. De knelpunten kunnen vervolgens ondergebracht worden onder drie grote noemers: (I) Versleuteling, (II) de bewaringsregimes en (III) toegang tot de bewaarde gegevens.

    Om te bepalen aan welke voorwaarden elk van deze belangrijkste onderdelen van de nieuwe Belgische dataretentiewet moeten voldoen om in overeenstemming te zijn met het Unierechtelijk kader, wordt er teruggegrepen naar het vorige hoofdstuk 3. Ten slotte wat betreft het onderzoeken van de conformiteit van deze elementen met het Unierechtelijk kader, werd er in

de eerste plaats gezocht naar bijdragen die de nieuwe wet analyseren. Om deze te vinden, werd voornamelijk de online databank Jurisquare geraadpleegd. Hieruit kwamen twee bijdragen voort die het vertrekpunt vormen van een eigen analyse. Daarnaast werd er in het kader van *Students@cuta* een gesprek georganiseerd met een van de medewerkers van het Coördinatieorgaan voor de dreigingsanalyse (OCAD). Een keer per jaar opent het OCAD namelijk zijn deuren om studenten de mogelijkheid te geven vragen te stellen aan de specialisten in het kader van hun masterscriptie. Dit gesprek heeft bijgedragen aan het uitwerken van de rol van het OCAD binnen de nieuwe Belgische dataretentiewet en het verfijnen van de analyse. Ten slotte werden ook andere documenten zoals policy documenten, adviezen van de Raad van State en de Gegevensbeschermingsautoriteit geraadpleegd om de analyse te ondersteunen. De beantwoording van subonderzoeksvraag 4 volgt uit deze analyse en wordt hernomen in de conclusie.

10. **AFBAKENING –** Het schrijven van een masterscriptie veronderstelt een goed afgebakend onderzoeksveld. Dit betekent dat het onderzoek niet alle aspecten van dataretentie uitgebreid kan weergeven. In hoofdstuk 2 vertaalt deze afbakening zich in het beschrijven van de voornaamste schijnargumenten binnen het veiligheid-versus-vrijheid-debat voor de behandeling van het onderwerp. Dit debat is echter omvangrijker en bestaat uit meer overwegingen en nuanceringen dan deze die beschreven worden in de masterscriptie. In hoofdstuk 3 werd er bewust gekozen om de arresten van het Hof van Justitie te filteren tot de zeven belangrijkste. De bewuste keuze om te focussen op de arresten van het Hof van Justitie impliceert ook dat de rol en de arresten van het Europees Hof voor de Rechten van de Mens niet worden geanalyseerd. Wat betreft hoofdstuk 4, moet erkend worden dat dataretentie bijvoorbeeld ook van belang is voor commerciële doeleinden van operatoren. Het speelt daarnaast ook een grote rol in de bewijsverzameling in strafzaken. Dit hoofdstuk beperkt zich tot de kernpunten die als belangrijk worden beschouwd in het licht van de arresten van het Hof van Justitie en het Grondwettelijk Hof. Dit brengt onvermijdelijk met zich mee dat de volledige impact van de nieuwe Belgische dataretentiewet op strafonderzoeken, de impact op de werking van operatoren en andere elementen van de nieuwe Belgische dataretentiewet niet of op summiere wijze behandeld worden. Ten slotte kan er meer gezegd worden over de geschiedenis van dataretentie in België, maar een uitvoerige bespreking hiervan zou niet bijdragen tot het oplossen van de onderzoeksvraag.

11. **STRUCTUUR –** De masterscriptie is zo opgebouwd dat er via een logische structuur een antwoord op de onderzoeksvraag kan bekomen worden. Na het uiteenzetten van het groter maatschappelijk kader waarbinnen dataretentie zich situeert, namelijk het veiligheid-versus-vrijheid-debat, wordt er overgegaan naar een analyse van de voorwaarden die voortkomen uit het Unierechtelijk kader. Deze twee delen dienen als basis voor het evaluatief gedeelte, waarbij de nieuwe Belgische dataretentiewet wordt getoetst aan de vastgestelde criteria. In de conclusie wordt er voorzien in een bonding antwoord op de onderzoeksvraag.

2. HET DILEMMA VEILIGHEID VERSUS VRIJHEID

2.1.Inleiding

12. **TOELICHTING HOOFDSTUK –** Dit hoofdstuk geeft het ruimer debat van veiligheid-versus-vrijheid weer waarin er wordt gestreefd naar het vinden van een evenwicht tussen het verzekeren van veiligheid enerzijds en het beschermen van fundamentele grondrechten anderzijds. Het is belangrijk om een notie te hebben van dit debat, aangezien dataretentie een inmenging teweegbrengt in de rechten en vrijheden van burgers. Dit doet namelijk vragen rijzen over de doelstelling en proportionaliteit ervan. Bij het nagaan van de nagestreefde doelstelling en zeker de invulling van de proportionaliteitsvereiste zal dit debat altijd uitwerking vinden. Om deze reden vormt dit hoofdstuk het breder maatschappelijk kader waarbinnen dataretentie moet begrepen worden en vormt het zo de basis voor de komende hoofdstukken.

13. **KADERING –** De bescherming van privacy in het huidig technologisch klimaat is een van de grote uitdagingen van de hedendaagse democratieën. Nieuwe technologieën geven de overheden niet alleen nieuwe vormen en manieren om haar taken uit te voeren, maar zij scheppen ook de mogelijkheid om in te grijpen in de persoonlijke levenssfeer van haar burgers.[3] Al jarenlang vormt de klassieke tweestrijd tussen veiligheid en privacy het onderwerp van juridische debatten. Hoewel privacy wordt erkend als een grondrecht van individuen en daarbij ook is vastgelegd in wetten en grondwetten, bestaat er aan de andere kant de noodzaak tot gegevensbewaring en -gebruik, een mechanisme dat bekend staat als dataretentie. Dit kunnen we linken aan twee bredere ontwikkelingen. Ten eerste bestaat er nu de technologie om grote hoeveelheden persoonsgegevens te verzamelen, op te slaan, te analyseren en met elkaar in verband te brengen.[4] Hierbij kan er verwezen worden naar onder andere clouddiensten, de vooruitgang in big data-technieken van commerciële bedrijven en geavanceerde technologische onderzoeksmethodes.[5] Ten tweede kan privacy worden misbruikt om illegaal of bedreigend gedrag, zoals georganiseerde misdaad en terroristische aanslagen, te verbergen.[6]

14. **VEILIGHEIDSUITDAGINGEN –** De wereldwijde veiligheidsuitdagingen na de terroristische aanslagen van 11 september 2001 hebben een revolutie teweeggebracht in de nationale aanpak van de strijd tegen bedreigingen van de openbare veiligheid.[7] "Veiligheid" werd opnieuw een belangrijk agendapunt. Het ruime en open concept van terrorisme heeft de Europese wetgever en nationale wetgevers in staat gesteld buitengewone maatregelen te nemen om deze ongedefinieerde bedreigingen het hoofd te bieden.[8] In het politieke klimaat van de "*war on terror"* werden de door aanbieders van telecommunicatiediensten verwerkte gegevens een waardevolle

[3] M. ZUBIK, P. PODKOWIK en R. RYBSKI (eds.), *European Constitutional Courts towards Data Retention Laws,* Zwitserland, Springer, 2021, vi.
[4] S.S. BOURDILLON, J. PHILIPS en M.D. RYAN, *Privacy vs. Security,* Londen, Springer, 2014, v.
[5] *Ibid.*
[6] *Ibid.*
[7] A. CAVOUKIAN, "Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head", *Health and technology* 2017, (329) 329.
[8] B. GRABOWSKA-MOROZ, "Data retention in the European Union", in M. ZUBIK, P. PODKOWIK en R. RYBSKI (eds.), *European Constitutional Courts towards Data Retention Laws,* Zwitserland, Springer, 2021, (3) 3.

bron van informatie voor rechtshandhavingsinstanties.[9] Het wetgevend activisme werd gevoed door de veronderstelling dat de inlichtingen- en wetshandhavingsdiensten niet in staat waren de "punten te verbinden" om de aanslagen te voorkomen.[10] Daarbij kwam de algemeen gedeelde overtuiging dat het bestaande wettelijke kader aanzienlijke veiligheidsgebreken vertoonde.[11] Deze ontwikkeling van de regelgeving geeft nog steeds aanleiding tot bezorgdheid over de eerbiediging van privacy en andere fundamentele rechten en vrijheden.

15. **ALTERNATIEVE WAARDEN** – Vaak wordt aangenomen dat privacy en veiligheid alternatieve waarden zijn, die niet samen kunnen worden nagestreefd.[12] Beide belangen zijn echter noodzakelijke voorwaarden voor een democratische samenleving en een werkbare symbiose is aangewezen. Er moet een evenwicht worden gevonden tussen het noodzakelijk bewaren van bepaalde data om misdrijven te bestrijden en voorkomen enerzijds en het waarborgen van privacy anderzijds. Om de belangen van privacy en veiligheid te kunnen afwegen, is het van cruciaal belang te beginnen met het definiëren van de concepten die in het geding zijn.

2.2. Concepten privacy en veiligheid

16. **CONCEPT PRIVACY –** Privacy is een begrip dat voortdurend in ontwikkeling is en niet los kan worden gezien van de technologische vooruitgangen.[13] Wat als privé wordt beschouwd en wat wettelijk als privé wordt beschermd, kan verschillen. Het houdt namelijk nauw verband met de menselijke waardigheid, de vrijheid en de onafhankelijkheid van het individu. Er zijn verschillende factoren die van invloed zijn op wat mensen als privé beschouwen en er bestaan grote verschillen tussen bepaalde samenlevingen en culturen.[14] Het hangt voornamelijk af van de concrete situatie: het delen van dezelfde informatie in verschillende situaties kan anders als privé worden beschouwd.[15] Een van de belangrijkste aandachtspunten betreffende de wettelijke bescherming van privacy is dat het niet mogelijk is één uitputtende juridische definitie te geven van het begrip. Privacy heeft een zeer lange geschiedenis; het vindt zijn oorsprong namelijk al in de oude samenlevingen. Het idee van privacy komt traditioneel voort uit het verschil tussen "privé" en "openbaar".[16] Natuurlijk verschillen de grenzen tussen privé en publiek al naar gelang het tijdperk en de samenleving, wat in de loop van de geschiedenis zal leiden tot de voortdurende verandering van wat mensen als privé beschouwen. Zelfs de Bijbel bevat enkele passages waarin de schending van de privacy in zijn vroege vorm naar voren kwam.[17] Vanuit juridisch oogpunt

[9] A. VEDASCHI, "Privacy versus Security: Regulating Data Collection and Retention in Europe. " in B.J. GOOLD en L. LAZARUS (eds.), *Security and Human Rights,* Londen, Hart Publishing, 2019, (275) 275.
[10] A. CAVOUKIAN, " Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head", *Health and technology* 2017, (329) 330.
[11] *Ibid.*
[12] S.S. BOURDILLON, J. PHILIPS en M.D. RYAN, *Privacy vs. Security,* Londen, Springer, 2014, 1.
[13] A. LUKACS, "What is Privacy? The History and Definition of Privacy." in G. Keresztes (ed), *Spring Wind 2016,* Budapest, Magyarország:Doktoranduszok Országos Szövetsége, 2016, (256) 256.
[14] C. FRIED, "Privacy", *The Yale Law Journal* 1968, (475) 475.
[15] H. NISSENBAUM, "Protecting Privacy in an Information Age: the Problem of Privacy in Public.", *Law and Philosophy* 1998, (559) 581.
[16] A. LUKACS, "What is Privacy? The History and Definition of Privacy." in G. Keresztes (ed), *Spring Wind 2016,* Budapest, Magyarország:Doktoranduszok Országos Szövetsége, 2016, 257.
[17] M.R. KONVITZ, "Privacy and the law: a Philosophical Prelude.", *Law and Contemporary Problems* 1966, (272) 272.

werden kwesties met betrekking tot het binnendringen in iemands huis reeds geregeld in de Codex van Hammurabi en het Romeinse recht.[18]

17. **JURIDISCHE INVULLING PRIVACY –** Op juridisch gebied is de eerste uitdrukkelijke erkenning ervan terug te voeren op het in 1980 gepubliceerde artikel *The Right to Privacy* van twee Amerikaanse juristen, BRANDEIS en WARREN, die het beroemde *right to be let alone* hebben uitgewerkt.[19] Zij herkenden twee fenomenen die een bedreiging vormden voor privacy: de technologische ontwikkeling en roddels, die een handel werden in kranten.[20] Gezien deze veranderingen waren zij de eersten die de erkenning eisten van het recht op privacy (dat zij definieerden als "het recht om met rust gelaten te worden") als een afzonderlijk en algemeen recht, als een recht dat bescherming bood tegen het louter emotionele lijden.[21] Een soortgelijke definitie wordt gegeven door DAVID FLAHERTY, die beweert dat privacy "het recht is om niet onnodig te worden gestoord".[22] Een haalbare definitie van privacy is geformuleerd door ALAN WESTIN: "Privacy is de aanspraak van individuen, groepen of instellingen om zelf te bepalen wanneer, hoe en in welke mate informatie over hen aan anderen wordt meegedeeld.[23] Sindsdien is het recht op privacy algemeen bekend en erkend, begon het zich te ontwikkelen en werd het een fundamenteel mensenrecht in Westerse samenlevingen.[24] Verschillende juristen hebben geprobeerd een definitie van privacy op te stellen, maar ondanks het feit dat de aanspraak op privacy universeel is, verschilt de concrete vorm ervan naar gelang van de heersende maatschappelijke overtuigingen en de economische en culturele omgeving.[25] Dit betekent dat privacy opnieuw moet worden geïnterpreteerd in het licht van de huidige tijd en moet worden onderzocht in de huidige context.

Vanaf de tweede helft van de 20e eeuw is het recht op privacy erkend als een fundamenteel mensenrecht van de eerste generatie in verschillende juridische documenten, zowel op internationaal niveau als op nationaal en regionaal niveau. Het recht op privacy kan onder andere worden teruggevonden in artikel 12 van de Universele Verklaring van de Rechten van de Mens, artikel 17 van het Internationaal verdrag inzake Burgerrechten en Politieke Rechten, artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM) en artikel 7 van het Handvest van de Grondrechten van de Europese Unie (hierna: EU-Handvest). Deze bepalingen geven echter geen specifieke aanwijzingen over wat privacy is of welke aspecten ervan wettelijk moeten worden beschermd. Hiervoor moet er gekeken worden naar de jurisprudentie. Het Europees Hof voor de Rechten van de Mens van de Raad van Europa (hierna: EHRM) en het Europees Hof van Justitie van de Europese Unie (hierna:

[18] D. SOLOVE, *Nothing to hide: the false tradeoff between privacy and security,* New Haven en Londen, Yale University Press, 2011, 4.
[19] B. BRATMAN, "Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy, *Tennessee Law Review* 2002, 623-652.
[20] S.D. WARREN en L.D. BRANDEIS, "The right to Privacy, *Harvard Law Review* 1890, (193) 193.
[21] *Ibid.*
[22] D. H. FLAHERTY, "On the Utility of Constitutional Rights to Privacy and Data Protection", *Case Western Reserve Law Review* 1991, (831) 831.
[23] A. WESTIN, *Privacy and Freedom*, New York, Atheneum, 1967, xvi + 487 p.
[24] A. LUKACS, "What is Privacy? The History and Definition of Privacy." in G. Keresztes (ed), *Spring Wind 2016,* Budapest, Magyarország:Doktoranduszok Országos Szövetsége, 2016, 256.
[25] *Ibid.,* 258.

HvJ) zijn de belangrijkste gerechtelijke instanties die bijdragen aan de bescherming van het recht op privacy.

18. **EVRM en EHRM –** Wanneer we spreken over privacy binnen het EVRM[26], moet er gekeken worden naar art. 8 EVRM. Het begrip "privéleven" heeft zich op relatief autonome wijze ontwikkeld onder auspiciën van het Europees Hof voor de Rechten van de Mens. In het algemeen heeft het Hof de werkingssfeer van artikel 8 EVRM ruim gedefinieerd, zelfs wanneer een specifiek recht niet in het artikel is opgenomen.[27] Ook de technologische en wetenschappelijke ontwikkelingen die zich na de aanneming van het EVRM hebben voorgedaan, hebben het EHRM ertoe aangezet een flexibele interpretatie van het privéleven onder de huidige omstandigheden te geven.[28] Bovendien verklaart de preambule van het EVRM niet alleen het behoud van deze grondrechten, maar ook de ontwikkeling ervan.[29] Het EHRM stelde in zijn rechtspraak dat inmenging in de volgende levensomstandigheden onder de reikwijdte van artikel 8 EVRM viel (en onderzocht verder of de inmenging al dan niet legitiem was omdat het geen absoluut recht is): Recht op afbeelding en foto's, publicatie van foto's, afbeeldingen en artikelen, bescherming van de persoonlijke reputatie; laster, gegevensbescherming, recht op toegang tot persoonlijke informatie, informatie over iemands gezondheid, verzamelen van bestanden of gegevens door veiligheidsdiensten of andere staatsorganen, toezicht door de politie, huisbezoeken, huiszoekingen en inbeslagnames, advocaat-cliënt relatie en privacy tijdens hechtenis en gevangenschap etc.[30] Benadrukt moet worden dat dit geen uitputtende lijst is. Het is onmogelijk het begrip privéleven te definiëren en precies aan te geven wat het inhoudt. Privacy is een fundamenteel mensenrecht dat inherent is aan de menselijke waardigheid en de autonomie van elke persoon en dat een persoonlijke sfeer biedt waarin mensen vrij kunnen denken en handelen. Europese wetenschappers en adviesraden onderstrepen ook dat privacy zeer moeilijk te definiëren is omdat "het privéleven een ruim begrip is dat niet uitputtend kan worden gedefinieerd" en "het begrip privéleven niet beperkt is tot een "inner circle"".[31] Bovendien stuiten pogingen om één enkele definitie van privacy te geven op de bewering dat "privacy" afhankelijk is van de cultuur van een land.

19. **EU-HANDVEST EN HVJ –** De arresten van het Europees Hof van Justitie worden sterk beïnvloed door het EHRM. Het EU-Handvest is geen verklaring van grondrechten en voorrechten met een universele werkingssfeer.[32] Artikel 51 van het EU-Handvest bepaalt dat het alleen van toepassing is op de EU-instellingen en de lidstaten wanneer zij zich bezighouden met de uitvoering van het EU-recht. Het EU-Handvest heeft dus tot doel de uitvoering en uitlegging van het EU-recht, met

[26] Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden van 4 november 1950, *BS* 19 augustus 1988, 5.029.
[27] EHRM 16 december 1992, nr. 13710/88, Niemietz/Duitsland, §29: "Het Hof acht het niet mogelijk of noodzakelijk om een uitputtende definitie van het begrip "privéleven" te geven.
[28] K. BLAY-GRABARCZYK, "Vie privée et nouvelles technologies", *RDLF* 2011, 1.
[29] A. LUKACS, "What is Privacy? The History and Definition of Privacy." in G. Keresztes (ed), *Spring Wind 2016,* Budapest, Magyarország:Doktoranduszok Országos Szövetsége, 2016, 260.
[30] EUROPEES HOF VOOR DE RECHTEN VAN DE MENS en RAAD VAN EUROPA, "Guide on Article 8 of the European Convention on Human Rights", 2022, www.echr.coe.int/documents/guide_art_8_eng.pdf.
[31] EHRM 25 september 2018, nr. 76639/11, Denisov/Oekraïne, §96.
[32] A. LUKACS, "What is Privacy? The History and Definition of Privacy." in G. Keresztes (ed), *Spring Wind 2016,* Budapest, Magyarország:Doktoranduszok Országos Szövetsége, 2016, 260.

inbegrip van de Algemene Verordening Gegevensbescherming (hierna: AVG), te sturen.[33] Het HvJ oordeelde dat het bewaren van privégegevens een beperking vormt op artikel 7 van het EU-Handvest en dat de toegang van nationale autoriteiten tot die gegevens een "afzonderlijke beperking op dat grondrecht" vormde, onder verwijzing naar de rechtspraak van het EHRM. De formulering van artikel 7 van het EU-Handvest was gebaseerd op artikel 8 van het EVRM. Het HvJ verwijst vele malen bewust naar de praktijk van het EHRM. Dit heeft tot gevolg dat de inhoud van het recht op privacy in grote mate gelijkloopt aan met de inhoud ervan uit de rechtspraak van het EHRM.[34]

20. **CONCEPT VEILIGHEID –** Vervolgens is het ook van cruciaal belang een onderscheid te maken tussen de termen nationale veiligheid, openbare veiligheid en terrorisme. Deze termen dekken namelijk allemaal een verschillende lading. Zoals later in deze masterscriptie zal worden uiteengezet, is de nagestreefde doelstelling een belangrijk element om te bepalen of een maatregel van gegevensbewaring is toegelaten.

Nationale veiligheid wordt gezien als synoniem voor staatsveiligheid. Het komt toe aan elke staat om dit begrip invulling te geven. Volgens de Dienst voor de Veiligheid van de Staat (hierna: VSSE) is de nationale veiligheid van België in het gedrang wanneer een of meerdere vitale belangen bedreigd worden.[35] Deze vitale belangen omvatten onder andere de rechtstaat, democratie, weerbaarheid en nationale waarden, fysieke veiligheid, territoriale integriteit, leefomgeving, economische welvaart, internationale orde en functionering van de EU.[36] Nationale veiligheid wordt ook steeds vaker via de digitale ruimte geraakt. De integriteit van de digitale ruimte maakt daarom deel uit van de fysieke en territoriale veiligheid en is tegelijkertijd ook verweven met alle veiligheidsbelangen.[37] De dreigingen ten aanzien van deze vitale belangen zijn van diverse aard. Dit kan gaan van oplopende spanningen tussen de grootmachten, terroristische en extremistische groeperingen tot georganiseerde misdaad en cybercriminaliteit.

Op EU-niveau vinden we het begrip **'openbare veiligheid'** terug in onder andere art. 4, lid 2 van het Verdrag betreffende de Europese Unie (hierna: VEU) en art. 15 lid 1 van de e-Privacy Richtlijn.[38] Deze wordt niet verder uitgewerkt, waardoor er moet gekeken worden naar de rechtspraak van het Hof van Justitie. Het behoort tot de vaste rechtspraak van het HvJ dat het begrip 'openbare veiligheid' zowel de interne als de externe veiligheid van een lidstaat dekt.[39] De openbare veiligheid kan in gevaar worden gebracht door de aantasting van het functioneren

[33] Verord. Europees Parlement en de Raad nr. 2016/679, 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 Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pb.L.* 4 mei 2016, afl. 119, 1.
[34] R. GELLERT en S. GURTWIRTH, "The Legal construction of privacy and data protection", *Computer Law and Security Review* 2013, (522) 524.
[35] VSSE, "Nationale veiligheidsstrategie",2021, www.premier.be/sites/default/files/articles/NVS_Online_NL.pdf, 9.
[36] *Ibid.*
[37] *Ibid.,* 10-11.
[38] Richtl. Europees Parlement en de Raad nr. 2002/58, 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), *Pb.L.* 31 juli 2002, afl. 201, 37.
[39] Zie onder andere HvJ 23 november 2010, nr. C-145/09, ECLI:EU:C:2010:708, Baden Württemberg/Panagiotis Tsakouridis.

van de instellingen en essentiële openbare diensten. Daarnaast kan de openbare veiligheid in gevaar worden gebracht wanneer het overleven van de bevolking, het risico van een ernstige verstoring van de externe betrekkingen, het risico van een ernstige verstoring van de vreedzame co-existentie of de aantasting van de militaire belangen een rol spelen. Wanneer we terugkeren naar het nationale niveau, kan er verwijzing worden gemaakt naar Titel VI. Misdaden en wanbedrijven tegen de openbare veiligheid binnen het Strafwetboek (hierna: Sw.).[40] Het gaat dan limitatief over verenigingen met het oogmerk een aanslag te plegen, de bedreiging met een aanslag of valse bommeldingen, het helpen ontvluchten van gevangenen, banbreuk en verberging van veroordeelde of vermoorde personen.

Ten slotte is het begrip **terrorisme** noodzakelijk voor het onderscheid. In artikel 8, 1°, b) van de wet van 30 november 1998 inzake de inlichtingen- en veiligheidsdienst (hierna: wet inlichtingendiensten) vinden we een wettelijke definitie van terrorisme.[41] Het wordt met name gedefinieerd als het gebruik van geweld tegen personen of materiële belangen om ideologische of politieke redenen met het doel zijn doelstellingen door middel van terreur, intimidatie of bedreigingen te bereiken. In uitvoering van het Kaderbesluit van de Raad van de Europese Unie van 13 juni 2002 inzake terrorismebestrijding werden bij wet van 19 december 2003 een aantal "terroristische misdrijven" strafbaar gesteld in de artikelen 137 tot en met 141 van het Strafwetboek. Artikel 137 §1 Sw. definieert het terroristisch misdrijf als volgt: "Als terroristisch misdrijf wordt aangemerkt het misdrijf bepaald in de paragrafen 2 en 3 dat door zijn aard of context een land of een internationale organisatie ernstig kan schaden en opzettelijk gepleegd is met het oogmerk om een bevolking ernstige vrees aan te jagen of om de overheid of een internationale organisatie op onrechtmatige wijze te dwingen tot het verrichten of het zich onthouden van een handeling, of om de politieke, constitutionele, economische of sociale basisstructuren van een land of een internationale organisatie ernstig te ontwrichten of te vernietigen." Deze terroristische misdrijven worden in de paragrafen 2 en 3 opgedeeld in twee categorieën, met name een aantal bestaande gemeenrechtelijke misdrijven waarvoor de incriminatie als "terroristisch misdrijf" bij toepassing van art. 138 §1 Sw. tot strafverzwaring leidt, en een aantal nieuwe misdrijven waarvan de straffen worden bepaald in art. 138, §2 Sw.

2.3. Debat veiligheid versus vrijheid

21. **VEILIGHEID VS. VRIJHEID –** Het debat over privacy en veiligheid is van grote waarde voor het vinden van het juiste evenwicht tussen beide belangen. Het vinden van dit evenwicht is niet alleen van belang op het wetgevingsniveau. Beslissingen over toezicht en gegevensverzameling worden op vele niveaus genomen, ook op praktisch en operationeel niveau. Veiligheid en privacy botsen vaak, maar er hoeft geen sprake te zijn van een nulsomafweging.[42] Wanneer dit debat wordt gehouden, zijn veiligheidsbelangen gemakkelijk te begrijpen aangezien er levens op het spel staan. Privacyrechten en -overwegingen zijn echter abstracter en vager. Veel mensen

[40] Strafwetboek van 8 juni 1867, *BS* 9 juni 1867, 3133.
[41] Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, *BS* 18 december 1998, 40312.
[42] A. CAVOUKIAN, "Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head", *Health and technology* 2017, (329) 330.

denken dat ze privacy moeten inruilen voor meer veiligheid. Tegelijkertijd voeren degenen aan de veiligheidskant van het debat krachtige argumenten aan om mensen ertoe aan te zetten deze ruil te accepteren. Met kennis van de onjuiste argumenten in het debat, over hoe de dataretentie werkt, en met pragmatische ideeën en oplossingen, is het mogelijk een productieve discussie te voeren over de balans tussen privacy en veiligheid.

22. **DEBAT –** Het is van belang om de belangrijkste onjuiste argumenten zowel aan de privacyzijde, als aan de veiligheidszijde in dit debat te identificeren om zo tot een werkbaar evenwicht te komen. In deze scriptie zullen de belangrijkste argumenten voor de behandeling van het onderwerp hieronder worden uitgewerkt. Ze allemaal identificeren zou het bestek van deze scriptie te buiten gaan.

23. **NIETS-TE-VERBERGEN-ARGUMENT –** Een eerste argument dat kan worden gefilterd uit dit debat is het "niets-te-verbergen"-argument. Deze wordt het beste samengevat met de zin: "Als je niks te verbergen hebt, heb je niks te vrezen."[43] Varianten van dit argument verschijnen vaak in blogs, sociale media, op televisie en andere fora. Deelnemers aan deze discussie proberen vaak het "niets te verbergen"-argument te weerleggen door te wijzen op dingen die mensen net wel willen verbergen. Wanneer dit argument wordt aangevoerd, is de onderliggende veronderstelling dat privacy gaat over het verbergen van slechte dingen. Privacy wordt als het ware beschouwd als een vorm van geheimhouding. Door die aanname te aanvaarden, nodigen we uit tot een onproductieve discussie over informatie die mensen waarschijnlijk zouden willen verbergen. Het "niets-te-verbergen"-argument komt namelijk voort uit de onjuiste vooronderstelling dat privacy gaat over het verbergen van een fout.[44] Het gaat uit van een bepaalde opvatting over wat privacy inhoudt en sluit andere perspectieven uit. Als we privacy daarentegen zien als een veelheid van zaken, dan blijkt dat de onthulling van slechte dingen slechts een van de vele problemen is die worden veroorzaakt door veiligheidsmaatregelen van de overheid.[45] Een voorbeeld dat deze stelling ondersteunt, is dat door het samenvoegen van kleine stukjes schijnbaar onschuldige gegevens, informatie veelzeggender wordt en de overheid informatie over burgers kan verzamelen.[46] Het is belangrijk hier een onderscheid te maken tussen twee manieren om een nationaal veiligheidsprogramma te rechtvaardigen dat toegang tot persoonlijke informatie eist. De eerste manier is om geen probleem te erkennen. Dit is hoe het niets-te-verbergen argument werkt. Het ontkent zelfs het bestaan van een probleem. De tweede manier om een dergelijk programma te rechtvaardigen is de problemen onderkennen, maar beweren dat de voordelen van het programma opwegen tegen het privacy-offer.[47] De eerste rechtvaardiging beïnvloedt de tweede, omdat de lage waarde die aan privacy wordt toegekend, gebaseerd is op een beperkte visie op het probleem. Het belangrijkste misverstand

[43] A. NIEUWENHUIS, "Review of Privacy vs. Security", *Utrecht Journal of International and European Law* 2015, (137) 138.
[44] D. SOLOVE, *Nothing to hide: the false tradeoff between privacy and security,* New Haven en Londen, Yale University Press, 2011, 21-22.
[45] *Ibid.,* 30.
[46] *Ibid.*
[47] *Ibid.,* 29

is dat het "niets te verbergen"-argument privacy op een bepaalde manier bekijkt, namelijk als het recht om dingen te verbergen.

24. **ALLES-OF-NIETS-ARGUMENT –** Ten tweede is er de alles-of-niets-denkfout. Het argument gaat dat veiligheid en privacy nooit met elkaar te verzoenen zijn.[48] Elke winst aan privacy betekent een verlies aan veiligheid, en omgekeerd. Dit uit zich in de gedachte dat privacy opgeven mensen veilig houdt. Maar het opofferen van privacy maakt ons niet automatisch veiliger en niet alle veiligheidsmaatregelen die kunnen genomen worden schenden de privacy.[49] Bovendien is er geen verband vastgesteld tussen de effectiviteit van een veiligheidsmaatregel en een overeenkomstige afname van privacy.[50] Met andere woorden, de meest effectieve veiligheidsmaatregelen hoeven niet de meest schadelijke te zijn voor privacyrechten. Veiligheid en privacy hoeven elkaar dus niet uit te sluiten. Een voorbeeld dat hierbij kan worden gegeven is het vergrendelen van de cockpitdeuren van vliegtuigen om te voorkomen dat een terrorist controle zou kunnen krijgen over het vliegtuig.

De alles-of-niets-redenering veroorzaakt een verstoring van het evenwicht tussen privacy en veiligheid. Wanneer veiligheid tegen privacy wordt afgewogen, moet de hele veiligheidsmaatregel niet worden afgewogen tegen de schade aan de privacy die het veroorzaakt. Als bijvoorbeeld rechterlijk toezicht en regelgeving ter bescherming van de privacy leiden tot vertragingen, papierwerk en beperkingen die een veiligheidsmaatregel 20 procent minder doeltreffend maken, heeft het geen zin de hele veiligheidsmaatregel af te wegen tegen de privacy. In plaats daarvan zou de afweging moeten gaan tussen privacy en de 20 procent geringere effectiviteit van de maatregel. De keuze is niet tussen een veiligheidsmaatregel en niets, maar tussen een veiligheidsmaatregel met toezicht en regulering en een veiligheidsmaatregel die uitsluitend door uitvoerende ambtenaren wordt bepaald. In veel gevallen doen toezicht en regelgeving geen wezenlijke afbreuk aan een veiligheidsmaatregel, zodat de kosten van de bescherming van de privacy vrij laag kunnen zijn. Helaas wordt het evenwicht zelden goed beoordeeld. Wanneer de balans wordt opgemaakt volgens de alles-of-niets-redenering, slaat de weegschaal drastisch door naar de beveiligingskant. De kosten van privacybescherming krijgen een minder zwaar gewicht toebedeeld en aan de veiligheidsmaatregel wordt te veel gewicht toegekend.

[48] A. NIEUWENHUIS, "Review of Privacy vs. Security", *Utrecht Journal of International and European Law* 2015, (137) 138.
[49] D. SOLOVE, *Nothing to hide: the false tradeoff between privacy and security,* New Haven en Londen, Yale University Press, 2011, 30.
[50] *Ibid.*

25. **KRITISCHE BENADERING –** Vervolgens bestaat er het probleem dat rechtbanken kunnen aarzelen om het oordeel van veiligheidsdeskundigen kritisch te benaderen wanneer ze het veiligheidscriterium evalueren en zoeken naar de balans tussen vrijheid en veiligheid.[51] De uitvoerende macht mag dan de aangewezen tak zijn om veiligheidsmaatregelen te ontwikkelen, helaas wordt zelden gemotiveerd waarom veiligheid niet op andere manieren kan worden bereikt en waarom een dergelijke veiligheidsmaatregel de beste is.[52] Het is aan de hoven en rechtbanken om een optimaal evenwicht te vinden tussen veiligheid en vrijheid. In onze constitutionele democratie heeft elke tak een rol te spelen bij het maken van beleid. De rechter beschermt de grondwettelijke rechten, niet als absolute beperkingen van het beleid van de uitvoerende en wetgevende macht, maar als belangrijke belangen die moeten worden afgewogen tegen de belangen van de regering. Voor een zinvolle afweging moet de rechter zowel het veiligheids- als het vrijheidsbelang onderzoeken. Als de rechter de doeltreffendheid van de veiligheidsmaatregelen niet in twijfel trekt, zal het veiligheidsbelang bijna altijd prevaleren. Dit kan ook vanuit een andere invalshoek bekeken worden. Als beleidsmakers weten dat ze hun beleid zullen moeten rechtvaardigen, zullen ze wellicht voorzichtiger zijn bij de keuze van hun beleid. Gerechtelijke controle zorgt ervoor dat veiligheidsfunctionarissen hun werk goed doen en verantwoording afleggen.

26. **MAATSCHAPPELIJKE WAARDE –** Ten slotte heeft privacy niet enkel individuele waarde, maar ook maatschappelijke waarde.[53] Traditioneel worden rechten vaak opgevat als bescherming van het individu tegen de inmenging van de maatschappij.[54] Veel theorieën over de waarde van privacy interpreteren privacy op deze manier. Zowel de nadruk op het individuele recht als de nadruk op individuele controle domineerden een groot deel van het juridische en filosofische denken over privacy aan het eind van de jaren 60 en in de jaren 80.[55] Dit was een tijd waarin informatie- en communicatietechnologieën de manieren veranderden waarop informatie werd verzameld, bewaard en geanalyseerd. Bij wijze van voorbeeld omschreef professor ALAN WESTIN privacy in zijn baanbrekende boek *Privacy and Freedom* in 1967 als het recht "van het individu om informatie over zichzelf te controleren".[56] In diezelfde periode begon zich een alternatieve, maar complementaire denkwijze over privacy te ontwikkelen.[57] Met name zagen sociologen privacy als onderdeel van een goed functionerende samenleving. Privacy is niet alleen waardevol voor het individu, maar ook voor de samenleving in het algemeen. Wanneer we individuele rechten beschermen, besluiten we als samenleving ons in te houden om de voordelen te ontvangen van het creëren van vrije zones waarin individuen zich kunnen ontplooien. Begin jaren 2000 groeide de belangstelling voor de maatschappelijke waarde, de rol en het belang van

[51] *Ibid.*, 41.
[52] *Ibid.,* 44.
[53] J. WAGNER DECEW, "The feminist critique of privacy: past arguments and new social understandings", in B. ROESSLER en D. MOKROSINKA (eds.), *Social Dimensions of Privacy, Interdisciplinary Perspectives,* Cambridge University Press, 2015, (85) 85.
[54] P.M. REGAN, "Privacy and the common good: revisited", in B. ROESSLER en D. MOKROSINKA (eds.), *Social Dimensions of Privacy, Interdisciplinary Perspectives,* Cambridge University Press, 2015, (50) 57.
[55] *Ibid.*, 53.
[56] A. WESTIN, *Privacy and Freedom*, New York, Atheneum, 1967, xvi + 487 p.
[57] P.M. REGAN, "Privacy and the common good: revisited", in B. ROESSLER en D. MOKROSINKA (eds.), *Social Dimensions of Privacy, Interdisciplinary Perspectives,* Cambridge University Press, 2015, (50) 55.

privacy.[58] Er kan bijvoorbeeld verwezen worden naar STEEVES, die zich baseerde op de vroegere geschriften van WESTIN, ALTMAN en GEORGE HERBERT MEAD om de sociale aspecten van privacy te heroveren.[59] Zij stelt dat privacy "een sociale constructie is die we creëren wanneer we dagelijks onderhandelen over onze relaties met anderen".

De samenleving beschermt privacy als middel om de orde in de gemeenschap te handhaven. Privacy is niet simpelweg een manier om individuen te bevrijden van sociale controle. Het is zelf een vorm van sociale controle die voortkomt uit de normen van een samenleving. Het is geen externe beperking van de samenleving, maar een interne dimensie van de samenleving. Daarom heeft privacy een sociale waarde. Privacy moet dus niet worden afgewogen als een individueel recht tegen het grotere maatschappelijke belang. Privacykwesties omvatten het afwegen van maatschappelijke belangen aan beide zijden van de schaal. Onder rechtsgeleerden, filosofen en sociale wetenschappers met belangstelling voor privacy is er een onmiskenbaar gevoel dat het passend, intellectueel verdedigbaar en essentieel is om privacy als een sociale waarde te beschouwen, gezien het verloop van de huidige bewakingsactiviteiten, of die nu plaatsvinden uit naam van de nationale veiligheid, terrorisme of de openbare veiligheid.[60]

[58] *Ibid.*
[59] V. STEEVES, "Reclaiming the Social Value of Privacy", in I. KERR , V. STEEVES en C. LUCOCK (eds.), *Lessons from the Identity Trail: Anonimity, Privacy and Identity in a Networked Society,* New York, Oxford University Press, 191-208.
[60] P.M. REGAN, "Privacy and the common good: revisited", in B. ROESSLER en D. MOKROSINKA (eds.), *Social Dimensions of Privacy, Interdisciplinary Perspectives,* Cambridge University Press, 2015, (50) 55.

2.4. Conclusie

27. **CONCLUSIE –** Hieruit kunnen we concluderen dat het uitgangspunt moet zijn dat de verhouding tussen veiligheid en privacy betekent dat ze elkaar in balans moeten houden. Deze balans is dynamisch. Veiligheid en privacy zijn beide nodig in een goed functionerende samenleving en ze vertegenwoordigen cruciale waarden in een democratische rechtsstaat. De opdracht voor de overheid en de samenleving bestaat erin om beide waarden te waarborgen. Het debat moet voortdurend worden gevoerd op een manier die recht doet aan beide kanten van de balans. Noch privacy, noch veiligheid kan ontbreken in een democratische rechtstaat. Aangezien beide nodig zijn, mag men zich niet verschuilen achter het privacybelang of veiligheidsbelang ter ondersteuning van het eigen standpunt. Privacy staat niet gelijk aan het verbergen van fouten en veiligheidsinstanties willen niet ten koste van de rechtstaat de veiligheid handhaven. Wie zich op slechts één van de zijden van de balans beroept, geeft daarmee aan slechts een deelbelang na te streven en niet het algemeen belang.

Bij de afweging tussen vrijheid en veiligheid moet er erkend worden dat veiligheidsinspanningen te allen tijde onderworpen zijn aan eisen van proportionaliteit, subsidiariteit en efficiëntie. Privacyinbreuken kunnen daarentegen gerechtvaardigd zijn wanneer aan de eisen van doeltreffendheid, noodzakelijkheid en proportionaliteit is voldaan. Privacy noch veiligheid heeft absolute waarde in de discussie. De bereidheid moet bestaan om de belangen aan beide zijden te erkennen en tegelijkertijd ook kritisch te staan tegenover de argumenten die worden aangevoerd. Er kan niet gestreefd worden naar de maximale realisatie van veiligheid of privacy. Streven naar maximilisatie van één van beide is ongewenst omdat daarmee het geheel van de balans in gevaar komt. Daarnaast streven beide waarden een gemeenschappelijk doel na. De samenleving beschermt privacy als middel om de orde in de gemeenschap te handhaven. Wanneer voorstellen worden gedaan met betrekking tot of rakend aan privacy of veiligheid, moet het andere belang er mee in betrokken worden.

Het is eigen aan een afweging tussen twee belangen, tussen rechtshandhaving en rechtsbescherming, tussen veiligheid en privacy, dat het bepalen van een evenwicht tot moeilijke (ethische) discussies kan leiden. De overheid zal keer op keer bij het vaststellen van maatregelen uitgedaagd worden om in eerste instantie na te denken over dit evenwicht en vervolgens dit tot uiting te laten komen in de uitwerking en handhaving ervan. Door in het debat beide waarden te erkennen waarvoor ze staan, drogredenen te kunnen identificeren en maatregelen uitgebreid te motiveren, geraken we steeds een stuk verder. Vervolgens is dezelfde taak aan de hoven en rechtbanken toebedeeld. Hoe dit concreet vorm zal moet krijgen, is echter nog niet duidelijk en zal afhankelijk zijn van geval tot geval, maar de roep om juridische oplossingen die eveneens praktisch haalbaar zijn, klinkt luider dan ooit.

3. HET UNIERECHTELIJK KADER

3.1. Inleiding

28. **TOELICHTING HOOFDSTUK –** In dit hoofdstuk worden de verschillende bewaarplichten geïdentificeerd op het niveau van de Europese Unie, samen met de doelstellingen die ze moeten nastreven en de voorwaarden waaraan ze moeten voldoen om gerechtvaardigd te zijn in een democratische samenleving. Dit gebeurt ten eerste door de relevante wetgeving binnen het primair en secundair EU-recht te bespreken. Vervolgens worden zeven arresten van het Hof van Justitie grondig geanalyseerd. Ieder arrest bevat een tussenconclusie die bijdraagt tot het vormen van de synthese. Deze synthese zal als uitgangspunt gebruikt worden om de conformiteit van de nieuwe Belgische dataretentiewet van 2022 met het Unierechtelijk kader in hoofdstuk 4 na te gaan.

3.2. Algemeen Europees wetgevend kader

29. **ART. 7 EN ART. 8 EU-HANDVEST -** Wat betreft het primair EU-recht, vormen artikel 7 en artikel 8 van het EU-Handvest[61] de belangrijkste bron. Artikel 7 waarborgt de eerbiediging van het privéleven en het familie- en gezinsleven. De in artikel 7 gewaarborgde rechten corresponderen met de rechten die in artikel 8 van het EVRM zijn gewaarborgd. Artikel 8 van het EU-Handvest waarborgt specifiek de bescherming van persoonsgegevens en is gebaseerd op de gegevensbeschermingsrichtlijn (nu: Algemene Verordening Gegevensbescherming[62]) alsmede op artikel 8 EVRM.

30. **ART. 52, LID 1 EU-HANDVEST -** De beperkingen op de uitoefening van deze rechten van het EU-Handvest zijn terug te vinden in artikel 52, lid 1, van het EU-Handvest. Volgens dit artikel moeten beperkingen bij wet worden gesteld en de wezenlijke inhoud van de rechten eerbiedigen. Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen op de uitoefening van de rechten en vrijheden worden toegelaten indien deze 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. Wat dit laatste betreft, bepaalt artikel 15, lid 1 van de e-Privacy Richtlijn[63] zelf dat de bewaring van gegevens "gerechtvaardigd" moet zijn door verwijzing naar een van de in artikel 15, lid 1, genoemde doelstellingen. Deze moet voor een "beperkte duur" gelden. De opsomming van doelstellingen is exhaustief. Daarnaast stelt hetzelfde artikel dat dergelijke maatregel "in een democratische samenleving noodzakelijk,

[61] Handvest van de Grondrechten van de Europese Unie van 12 december 2007, *Pb.L.* 26 oktober 2012, afl. 326, 391.
[62] Verord. Europees Parlement en de Raad nr. 2016/679, 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 Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pb.L.* 4 mei 2016, afl. 119, 1. Hierna: Algemene Verordening Gegevensbescherming of AVG.
[63] 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), *OJ L* 201, 31.7.2002, p. 37–47. Hierna: "e-Privacy Richtlijn"

redelijk en proportioneel moet zijn". Overweging 11 van de e-Privacy Richtlijn preciseert dat maatregelen die afwijken van de beginselen "strikt" evenredig moeten zijn aan het beoogde doel.

31. **DATARETENTIERICHTLIJN -** In 2006 nam de Europese Unie (hierna: EU) de dataretentierichtlijn[64] aan. De dataretentierichtlijn strekte tot harmonisatie van de nationale verplichtingen van aanbieders van openbare elektronische communicatiediensten en -netwerken met betrekking tot het bewaren van bepaalde gegevens, hoofdzakelijk identificatie-, verkeers- en locatiegegevens in verband met communicatie.[65] Identificatiegegevens omvatten de gegevens die erop gericht zijn iemands identiteit vast te stellen, bijvoorbeeld iemands naam, voornaam, geboortedatum en rijksregisternummer. Verkeersgegevens zijn gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan.[66] Een voorbeeld hiervan zijn gebelde nummers en de bijbehorende tijdstippen, alsook duur van de gevoerde gesprekken. Locatiegegevens zijn ten slotte gegevens die worden verwerkt in een elektronische-communicatienetwerk waarmee de geografische positie van de eindapparatuur van een gebruiker van een algemeen beschikbaar elektronische-communicatiedienst wordt aangegeven.[67] De roep om harmonisatie op dit gebied kwam oorspronkelijk voort uit de bomaanslagen op treinen in Madrid in maart 2004 en de aanslagen in Londen op 7 juli 2005.[68] De richtlijn is op 15 maart 2006 door het Europees Parlement en de Raad aangenomen en de tekst van de richtlijn is vervolgens in april 2006 in het Publicatieblad bekendgemaakt.

Er werden drie redenen aangegeven voor deze Europese dataretentieregeling. Ten eerste belemmerden de juridische en technische verschillen tussen de nationale bepalingen op het gebied van het bewaren van gegevens ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten de werking van de interne markt voor elektronische communicatie.[69] De aanbieders van diensten worden immers geconfronteerd met uiteenlopende voorschriften wat betreft de categorieën van de te bewaren verkeers- en locatiegegevens, de bewaringsvoorwaarden en bewaringstermijnen.[70] De toenemende invloed van digitalisering heeft de verscheidenheid aan nationale regels des te problematischer gemaakt. Internetoperatoren en -dienstenaanbieders opereren niet langer binnen nationale grenzen, maar bieden hun diensten eenvoudig aan binnen de cyberspace.[71] Dit kan het voor pan-Europese of buitenlandse spelers bemoeilijken om hun digitale diensten op de nationale markt aan te bieden als elk land andere regels hanteert over welke data moet worden bijgehouden, op welke manier en hoe lang.[72] Ten

[64] Richtl. Europees Parlement en de Raad nr. 2006/24, 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, *Pb.L.* 13 april 2006, afl. 105, 54. Hierna "dataretentierichtlijn".
[65] Preambule overw.21 dataretentierichtlijn.
[66] Art. 2, lid 2, b) e-Privacy Richtlijn.
[67] Art. 2, lid 2, c) e-Privacy Richtlijn.
[68] E. CELESTE, " The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios", *European Constitutional Law Review* 2019, (134) 136.
[69] Preambule overw. 6 dataretentierichtlijn.
[70] *Ibid.*
[71] C. VAN DE HEYNING, "Het moeilijke evenwicht tussen privacy & veiligheid: De impact van het debat over bewaren van communicatiegegevens", *Radices* 2022, (132) 133.
[72] *Ibid.*

tweede meende de Europese Unie dat een harmonisatie van de regels ook nodig was voor de bescherming van de privacy en persoonsgegevens. De Europese Unie had reeds secundaire regelgeving uitgewerkt met betrekking tot de verwerking van persoonsgegevens, namelijk de Algemene Verordening Gegevensbescherming, en meer specifiek over de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, met name de e-Privacy Richtlijn. Deze regels concretiseren de bescherming van het privéleven en persoonsgegevens in de sector van elektronische- en telecommunicatie. Ten derde erkende de Europese Unie dat de bewaring van gegevens een noodzakelijk en doeltreffend onderzoeksinstrument is voor wetshandhaving in verschillende lidstaten, en met name bij ernstige aangelegenheden zoals georganiseerde misdaad en terrorisme, dient gezorgd te worden dat de bewaarde gegevens beschikbaar zijn voor de wetshandhavingsautoriteiten gedurende een bepaalde periode, onder specifieke voorwaarden.[73] De richtlijn moest dan ook het gebruik van communicatiegegevens mogelijk maken, binnen een kader van de bescherming van persoonsgegevens en privacy.

32. **DIGITAL RIGHTS IRELAND -** In 2014 verklaarde het Hof van Justitie van de Europese Unie de dataretentierichtlijn ongeldig in het arrest *Digital Rights Ireland*.[74] Het Hof stelde dat de richtlijn in kwestie onverenigbaar is met het recht op eerbiediging van het privéleven en op bescherming van persoonsgegevens, zoals gewaarborgd door de artikelen 7 en 8 van het EU-Handvest.[75] De dataretentierichtlijn streefde weliswaar een legitiem doel na, namelijk de bestrijding van zware criminaliteit, maar doorstond de evenredigheidstoets niet.[76] Concreet stelde het Hof dat het verzamelen van verkeers- en locatiegegevens van alle burgers om criminaliteit te bestrijden, een onevenredige inbreuk op hun rechten vormt en daarom in strijd is met het Unierecht. Een dergelijke bewaring is enkel mogelijk als er objectieve redenen zijn voor die bewaring, bijvoorbeeld omdat er voor een persoon aanwijzingen bestaan, zelfs indirect, dat er een verband is met zware criminaliteit.[77] Het algemeen bewaren van elektronische communicatiegegevens zonder differentiatie houdt in dat de meeste opgeslagen gegevens afkomstig zijn van personen die geen betrokkenheid hebben bij criminele of gevaarlijke activiteiten voor de staat.[78] Daardoor mist er een verantwoording om de bescherming van de privacy en persoonsgegevens van deze personen te beperken door hun communicatie bij te houden.[79] Het Hof benadrukte dat naast deze rechten, een algemene dataretentie ook de vrijemeningsuiting ondermijnt, omdat mensen zich meer bewust worden van wat ze naar wie communiceren en zelfcensuur toepassen.[80] Een algemene dataretentieplicht kan daarom een "chilling effect" hebben op de vrijemeningsuiting. Dit kan vooral van invloed zijn op tegenstanders van het overheidsbeleid, mensenrechtenverdedigers en minderheden.

[73] Preambule overw. 9 dataretentierichtlijn.
[74] HvJ (Grote kamer) 8 april 2014, nrs. C-293/12 en C-594/12, ECLI:EU:C:2014:238, Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a. en Kärntner Landesregierung e.a. Hierna: Digital Rights Ireland.
[75] *Ibid*, overw. 73.
[76] *Ibid*, overw. 37, 44 en 59-69.
[77] C. VAN DE HEYNING, "Het moeilijke evenwicht tussen privacy & veiligheid: De impact van het debat over bewaren van communicatiegegevens", *Radices* 2022, 136.
[78] *Ibid.*
[79] Digital Rights Ireland, overw. 28.
[80] *Ibid*.

33. **AVG EN E-PRIVACY RICHTLIJN -** Dit betekent dat op wetgevend niveau de belangrijkste bronnen de Algemene Verordening Gegevensbescherming en de e-Privacy Richtlijn betreffen. De AVG, ook bekend onder de Engelse afkorting GDPR, heeft als doel om de grondrechten van de burgers in het digitale tijdperk te versterken en het handelsverkeer te bevorderen door de regels voor bedrijven in de digitale eengemaakte markt te verduidelijken.[81] Deze verordening heeft een einde gemaakt aan de versnippering die het gevolg was van uiteenlopende nationale systemen. Het is op 24 mei 2016 in werking getreden en is sinds 25 mei 2018 van toepassing. De e-Privacy Richtlijn harmoniseert de regelgeving van de lidstaten die nodig is om een gelijk niveau van bescherming van fundamentele rechten en vrijheden - met name het recht op een persoonlijke levenssfeer - bij de verwerking van persoonsgegevens in de sector elektronische communicatie te waarborgen en om te zorgen voor het vrij verkeer van dergelijke gegevens en van elektronische-communicatieapparatuur en -diensten in de Gemeenschap.[82] Hoewel er een overlap is tussen de materiële toepassingsgebieden van de e-Privacy Richtlijn en de AVG, betekent dit niet automatisch dat de regels in strijd zijn met elkaar. Dit wordt niet alleen duidelijk bij het vergelijken van de verschillende bepalingen, maar ook door artikel 1, lid 2 van de e-Privacy Richtlijn, waarin wordt aangegeven dat de bepalingen van deze richtlijn een aanvulling vormen op AVG. Sommige bepalingen van de e-Privacy Richtlijn specificeren de regels van de AVG met betrekking tot de verwerking van persoonsgegevens in de sector van elektronische communicatie. Volgens het principe van *lex specialis derogate legi generali* hebben specifieke bepalingen voorrang op algemene regels in de situaties die zij specifiek regelen.[83] Als de e-Privacy Richtlijn de regels van de AVG specificeert, hebben de specifieke bepalingen van de e-Privacy Richtlijn voorrang op de algemene bepalingen van de AVG. Voor elke verwerking van persoonsgegevens waarop de e-Privacy Richtlijn niet specifiek van toepassing is, blijven de bepalingen van de AVG van toepassing. De e-Privacy Richtlijn vult ook de bepalingen van de AVG aan met betrekking tot de verwerking van persoonsgegevens in de sector van elektronische communicatie.[84] Sommige bepalingen van de e-Privacy Richtlijn zijn bedoeld om abonnees en gebruikers van openbare elektronische-communicatiediensten te beschermen. De abonnees kunnen zowel natuurlijke als rechtspersonen zijn. Door de AVG aan te vullen, beschermt de e-Privacy Richtlijn niet alleen de fundamentele rechten van natuurlijke personen, zoals hun recht op bescherming van de persoonlijke levenssfeer, maar ook de rechtmatige belangen van rechtspersonen.[85]

34. **E-PRIVACY VERORDENING -** De e-Privacy Verordening moet de e-Privacy Richtlijn vervangen. De e-Privacy Verordening is in de eerste plaats gericht op bedrijven die actief zijn in de digitale economie en specificeert aanvullende eisen waaraan zij moeten voldoen met betrekking tot de

[81] Preambule overw. 101 AVG en art. 1, lid 2 AVG.
[82] Art. 1 e-Privacy Richtlijn.
[83] EDPS, "Advies 5/2019 over de wisselwerking tussen de e- privacyrichtlijn en de algemene verordening gegevensbescherming, met name wat betreft de taken en bevoegdheden van gegevensbeschermingsautoriteiten", 12 maart 2019, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_nl, 16.
[84] *Ibid*.
[85] *Ibid*, 17.

verwerking van persoonsgegevens.[86] Aangezien er over de huidige tekst van de verordening enkele twistpunten bestaan, vorderen deze echter niet zo snel als het Portugese voorzitterschap recentelijk naar voren heeft geschoven. De e-Privacy Verordening zal naar verwachting zeker niet vóór medio of eind 2023 in werking treden. Een mogelijke overgangsperiode van 24 maanden betekent dat eventuele nieuwe verordening zelfs niet vóór medio of eind 2025 in werking zou treden.

35. **ARRESTEN HOF VAN JUSTITIE** - In navolging van het *Digital Rights Ireland*-arrest werd het Hof van Justitie intussen reeds verschillende malen opnieuw bevraagd over de bewaring van telecommunicatiegegevens in de strijd tegen criminaliteit. In deze datareteniesaga probeert het Hof van Justitie een evenwicht te vinden tussen het beschermen van fundamentele rechten en het waarborgen van nationale veiligheid en de strijd tegen criminaliteit. Onder "titel 1.2 rechtspraak van het Hof van Justitie" volgt een analyse van de belangrijkste arresten waarin het Hof van Justitie haar rechtspraak over de toelaatbaarheid van de bewaring van elektronische communicatiegegevens alsook het gebruik en de toegang daartoe verder probeert te verduidelijken. Het gaat met name over de arresten: (I) Tele2 Watson (2016)[87], (II) Ministerio Fiscal (2016)[88], (III) La Quadrature du net (2020)[89], (IV) Privacy International (2020)[90], (V) Prokuratuur[91], (VI) Commissioner of An Garda Síochána (2022)[92] en (VII) SpaceNet en VD (2022)[93].

[86] EUROPEES PARLEMENT, "Proposal for a regulation on privacy and electronic communications", 20 april 2023, www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform.
[87] HvJ (Grote kamer) 21 december 2016, nrs. C-203/15 en C-698/15, ECLI:EU:C:2016:970, Tele2 Sverige AB/Post-och telestyrelsen en Secretary of State for the Home Department/Tom Watson e.a. Hierna: Tele 2 Watson.
[88] HvJ (Grote kamer) 2 oktober 2018, nr. C-207/16, ECLI:EU:C:2018:788, Ministerio Fiscal. Hierna: Ministerio Fiscal.
[89] HvJ (Grote kamer) 6 oktober 2020, nrs. C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, La Quadrature du Net e.a./Premier ministre e.a., French Data Network e.a. en Ordre des barreaux francophones et germanophone e.a./Conseils des ministres. Hierna: La Quadrature du Net.
[90] HvJ (Grote kamer) 6 oktober 2020, nr. C-623/17, ECLI:EU:C:2020:790, Privacy International/Secretary of State for Foreign and Commonwealth Affairs e.a. Hierna: Privacy International
[91] HvJ (Grote kamer) 2 maart 2021, nr. C-746/18, ECLI:EU:C:2021:152, H.K. Prokatuur. Hierna: Prokuratuur.
[92] HvJ (Grote kamer) 5 april 2022, nr. C-140/20, ECLI:EU:C:2022:258, Commissioner of An Garda Síochána. Hierna: Commissioner of An Garda Síochána.
[93] HvJ (Grote kamer) 20 september 2022, nr. C-793/19 en C-794/19, ECLI:EU:C:2022:702, SpaceNet en Telekom Deutschland. Hierna: SpaceNet.; HvJ (Grote Kamer) 20 september 2022, nr. C-339/20, ECLI:EU:C:2022:703, VD. Hierna: VD.

3.3. Rechtspraak van het Hof van Justitie

3.3.1. C-203/15 – Tele2 Watson

36. **FEITEN –** Het arrest vloeit voort uit twee afzonderlijke verwijzingen naar artikel 267 VWEU met betrekking tot de interpretatie van het *Digital Rights Ireland* arrest.[94] De eerste verwijzing heeft betrekking op Tele2 Sverige AB, een Zweedse provider van elektronische communicatie.[95] Tele2 Sverige weigerde elektronische communicatiegegevens op te slaan nadat de dataretentierichtlijn ongeldig was verklaard in de *Digital Rights Ireland*-zaak.[96] Er ontstond een geschil over de interpretatie van het arrest waardoor de Zweedse minister van Justitie opdracht gaf tot het opmaken van een rapport om de verenigbaarheid van de Zweedse wetgeving met de EU-wetgeving en het EVRM te beoordelen.[97] Dit verslag concludeerde dat het arrest *Digital Rights Ireland* niet kan worden uitgelegd als een principieel verbod op algemene en ongedifferentieerde bewaring van gegevens, noch als een vaststelling van criteria - die allemaal vervuld moeten zijn - om wetgeving als evenredig te beschouwen. Volgens het verslag moeten alle omstandigheden worden beoordeeld om de verenigbaarheid van de Zweedse wetgeving met de EU-wetgeving te bepalen.[98] Tele2 Sverige stelde dat het rapport op een verkeerde interpretatie van het arrest was gebaseerd, waardoor de verwijzende rechter het Hof van Justitie verzocht om zich uit te spreken over de vraag of de algemene en ongedifferentieerde bewaring van elektronische communicatiegegevens op zich onverenigbaar is met de artikelen 7, 8 en 52, lid 1, van het EU-Handvest.[99] Het tweede verzoek, genaamd Watson, werd gedaan door het Court of Appeal in het kader van verzoeken om rechterlijke toetsing van de Britse Data Retention and Investigatory Powers Act (hierna: DRIPA) op grond van onverenigbaarheid met het EU-Handvest en het EVRM.[100] De verwijzende rechter betwistte of het *Digital Rights Ireland* - arrest "dwingende vereisten van EU-recht" bevatte die de nationale wetgeving inzake de bewaring en toegang tot communicatiegegevens moesten respecteren.[101] De nationale rechter oordeelde dat een onderscheid moest worden gemaakt tussen wetgeving inzake bewaring en wetgeving inzake toegang. Het Court of Appeal vroeg het Hof van Justitie om te onderzoeken of het arrest in kwestie dwingende vereisten van Unierecht bevat die van toepassing zijn op de regeling van de toegang tot bewaarde gegevens op nationaal niveau.[102]

37. **ANALYSE VAN HET HOF -** Het Hof onderzoekt vooreerst of de nationale wetgeving inzake de bewaring van en toegang tot verkeers- en locatiegegevens binnen de werkingssfeer van de e-Privacy Richtlijn valt. Het Hof heeft daarbij de algemene structuur van de richtlijn gevolgd om te concluderen dat dit weldegelijk het geval is. Ondanks de formulering van artikel 1, lid 3, van de e-Privacy Richtlijn was het Hof niettemin van oordeel dat artikel 15, lid 1, van deze richtlijn "noodzakelijkerwijs veronderstelt dat de daarin bedoelde nationale maatregelen, zoals die

[94] C. FORGET, "L'obligation de conservation des "métadonnées": la fin d'une longue saga juridique?", *Journal des Tribunaux* 2017, (233) 238.
[95] Tele 2 Watson, overw. 44.
[96] J. MEESE, "Dataretentie: het Hof van Justitie waakt over onze privacy", *RWE* 2016-17, (1639) 1639.
[97] Tele2 Watson, overw. 17.
[98] *Ibid*.
[99] *Ibid.*, Overw. 46-47.
[100] *Ibid.*, overw. 56.
[101] *Ibid*.
[102] *Ibid.*, overw. 59.

betreffende de bewaring van gegevens met het oog op de bestrijding van criminaliteit, binnen de werkingssfeer van deze richtlijn vallen, aangezien het de lidstaten uitdrukkelijk toestaat deze slechts vast te stellen indien aan de in de richtlijn gestelde voorwaarden is voldaan".[103] Bovendien, aangezien de bewaring van gegevens uitsluitend gebeurt om de bevoegde nationale autoriteiten toegang te kunnen geven tot die gegevens, impliceert een nationale regeling die voorziet in de bewaring van gegevens in beginsel ook bepalingen betreffende de toegang van de bevoegde nationale autoriteiten tot die bewaarde gegevens.[104]

Belangrijker is de vraag of een algemene en ongedifferentieerde gegevensbewaring verenigbaar is met artikel 15, lid 1 van de e-Privacy Richtlijn, gelet op de artikelen 7, 8 en 52, lid 1, van het EU-Handvest. Het Hof start zijn analyse door te benadrukken dat de hoofddoelstelling van de e-Privacy Richtlijn erin bestaat om in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het EU-Handvest bedoelde rechten te waarborgen[105] en gebruikers van elektronische communicatiediensten bescherming te bieden tegen de risico's die de technologische vooruitgang met zich meebrengt voor de grondrechten[106]. Krachtens artikel 5, lid 1, van de e-Privacy Richtlijn zijn lidstaten verplicht het vertrouwelijk karakter van de communicatie en de daarmee verband houdende verkeersgegevens te garanderen. Hoewel artikel 15, lid 1, van de e-Privacy Richtlijn de lidstaten toelaat de draagwijdte van het vertrouwelijk karakter van de communicatie en van de daarmee verband houdende verkeersgegevens te beperken, moet het volgens de vaste rechtspraak van het Hof echter strikt worden uitgelegd.[107] Het Hof benadrukte ook dat volgens de bewoordingen van artikel 15, lid 1, de maatregelen in overeenstemming moeten zijn met de algemene beginselen van het Unierecht, met inbegrip van de grondrechten in het EU-Handvest.[108] Onder verwijzing naar zijn eerdere rechtspraak wees het Hof ook op het belang van de betrokken grondrechten in de huidige context, namelijk het recht op privacy (artikel 7 EU-Handvest), het recht op gegevensbescherming (artikel 8 EU-Handvest) en het recht op vrijheid van meningsuiting (artikel 11 EU-Handvest).[109]

38. Nadat het Hof de draagwijdte van de bewaarplicht had vastgesteld, wordt de onthullende aard van deze gegevens benadrukt en herinnert het Hof tegelijk aan zijn conclusie in de zaak *Digital Rights Ireland*. Deze stelde dat uit deze gegevens, in hun geheel beschouwd, "zeer precieze conclusies kunnen worden getrokken over het privéleven van de personen wier gegevens zijn bewaard".[110] Aan de hand van deze gegevens kan het profiel van de betrokken personen worden

[103] *Ibid,* Overw. 73.
[104] *Ibid,* Overw. 79.
[105] Tele 2 Watson, overw. 82.
[106] Tele 2 Watson, overw. 83.
[107] Tele 2 Watson, overw. 89.; D. BIJNENS, "De wetgeving inzake dataretentie: *the saga continues…*" (noot onder HvJ 21 december 2018, gevoegde zaken nrs. C-203/15 en C-698/15, ECLI:EU:C:2016:970, *Tele2 Sverige AB* en *Secretary of State for the Home Department*), *TBP* 2017, (525) 526.
[108] Tele 2 Watson, overw. 91.; Zie naar analogie HvJ 20 mei 2003, nrs. C-465/00, C-138/01 en C-139/01, EU:C:2003:294, Österreichischer Rundfunk e.a., overw. 68; HvJ 13 mei 2014, nr. C-131/12, EU:C:2014:317, Google Spanje en Google, overw. 68, en HvJ 6 oktober 2015, nr. C-362/14, EU:C:2015:650, Schrems, overw. 38.
[109] Tele 2 Watson, overw. 92-93.; D. BIJNENS, "De wetgeving inzake dataretentie: *the saga continues…*" (noot onder HvJ 21 december 2018, gevoegde zaken nrs. C-203/15 en C)698/15, ECLI:EU:C:2016:970, *Tele2 Sverige AB* en *Secretary of State fort he Home Department*), *TBP* 2017, (525) 526.
[110] Tele 2 Watson, overw. 98.

bepaald, informatie die, wat het recht op bescherming van het privéleven betreft, even gevoelig is als de inhoud zelf van de communicatie.[111] Een algemene en ongedifferentieerde regeling inzake gegevensbewaring vormt dan ook een bijzonder ernstige inbreuk op het recht op privacy en gegevensbescherming en daardoor kan de betrokken gebruiker waarschijnlijk het gevoel krijgen dat zijn privéleven voortdurend wordt in de gaten gehouden.[112] Daarenboven erkende het Hof dat ook het gebruik van elektronische communicatiemiddelen en dus de uitoefening door de gebruikers van hun vrijheid van meningsuiting kan aangetast worden.[113] Om deze redenen oordeelde het Hof dat, gelet op de ernst van deze ingreep in de betrokken grondrechten ter bestrijding van criminaliteit, alleen het doel om ernstige criminaliteit te bestrijden een nationale wetgeving inzake de bewaring van verkeersgegevens en locatiegegevens kan rechtvaardigen.[114]

Het Hof erkende weliswaar dat de bestrijding van ernstige criminaliteit voor haar doeltreffendheid afhankelijk kan zijn van moderne opsporingstechnieken, maar deze doelstelling op zich niet kan rechtvaardigen dat een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens noodzakelijk is voor deze misdaadbestrijding.[115] Hiervoor steunt het Hof op twee grote redenen. Ten eerste vereist een dergelijke wetgeving geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van openbare veiligheid. Zij beperkt de bewaring met name niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaald geografisch gebied en/of een kring van personen die op een of andere wijze betrokken kunnen zijn bij een ernstig strafbaar feit, of op personen van wie de bewaring van de gegevens om andere redenen kunnen helpen bij de bestrijding van criminaliteit.[116] Ten tweede stelt het Hof dat een dergelijke regeling tot gevolg heeft dat de bewaring van verkeersgegevens en van de locatiegegevens de regel is, terwijl de e-Privacy Richtlijn vereist dat deze bewaring van gegevens de uitzondering vormt.[117]

Als gevolg van deze tekortkomingen oordeelde het Hof dat de nationale regeling de grenzen van het strikt noodzakelijke overschrijdt en niet kan worden beschouwd als gerechtvaardigd op grond van artikel 15, lid 1 van de e-Privacy Richtlijn gelezen in het licht van het EU-Handvest.[118] Het Hof ging echter niet zo ver dat het alle bewaring van gegevens onrechtmatig achtte. Het benadrukte dat artikel 15, lid 1 van de e-Privacy Richtlijn een lidstaat niet belet een regeling in te voeren die het mogelijk maakt verkeers- en locatiegegevens gericht te bewaren met het oog op de preventieve bestrijding van zware criminaliteit.[119] Die wetgeving moet echter beperkt blijven tot wat strikt noodzakelijk is in termen van de categorieën bewaarde gegevens, de

[111] Tele 2 Watson, overw. 99.; I. CAMERON, "Balancing data protection and law enforcement needs: Tele2 Sverige and Watson", *CML Rev.* 2017, (1467) 1478.
[112] Tele 2 Watson, overw. 100.
[113] Tele 2 Watson, overw. 101.; M. PANZAVOLTA, S. ROYER en H. SEVERIJNS, "Algemene dataretentie: ten minste houdbaar tot…?", *T. Strafr.* 2018, (3) 10.
[114] Tele 2 Watson, overw. 102.; T. VAN CANNEYT, A. BERTRAND, S. CROUZET en L. VANDERDONCKT, "Data Protection: CJEU case law review 1995-2020, *Computerrecht* 2021, (78) 137.
[115] Tele 2 Watson, overw. 103.
[116] Tele 2 Watson, overw. 106.; Tele 2 Watson, overw. 101.; M. PANZAVOLTA, S. ROYER en H. SEVERIJNS, "Algemene dataretentie: ten minste houdbaar tot…?", *T. Strafr.* 2018, (3) 10.
[117] Tele 2 Watson, overw. 104.
[118] C. VAN DE HEYNING, "Het moeilijke evenwicht tussen privacy & veiligheid: De impact van het debat over bewaren van communicatiegegevens", *Radices* 2022, (132) 137.; Tele 2 Watson, overw. 107.
[119] C. CONINGS en S. ROYER, "Ook hervormde dataretentiewet staat onder druk", *Juristenkrant* 2017, (1) 1.

betrokken communicatiemiddelen, de personen en de betrokken periode.[120] Een dergelijke regeling moet met name aangeven "in welke omstandigheden en onder welke voorwaarden" een maatregel van gegevensbewaring als preventieve maatregel kan worden genomen.[121] Het Hof benadrukte ook dat, hoewel de precieze contouren kunnen verschillen, de bewaring van gegevens moet voldoen aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel.[122] De nationale regeling moet dus gebaseerd zijn op bewijs: dit objectieve bewijs moet het mogelijk maken "een publiek te identificeren van wie de gegevens een verband, althans een indirect verband, met ernstige strafbare feiten kunnen aantonen".[123]

39. Vervolgens ging het Hof over tot de tweede prejudiciële vraag in Tele2 (die in wezen dezelfde was als de eerste vraag in Watson), namelijk of dezelfde Unierechtelijke bepalingen zich eveneens verzetten tegen een nationale regeling die de toegang van de bevoegde nationale autoriteiten tot de bewaarde communicatiegegevens regelt (I) zonder te bepalen dat die toegang alleen wordt verleend ter bestrijding van ernstige criminaliteit, (II) dat die toegang aan een voorafgaand toezicht door de rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit is onderworpen, en (III) dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard.

Het Hof herhaalde dat de toegang tot bewaarde gegevens beperkt is overeenkomstig de limitatief opgesomde doelstellingen in artikel 15, lid 1, van de e-Privacy Richtlijn, en dat alleen de doelstelling van bestrijding van ernstige criminaliteit deze toegang rechtvaardigt.[124] Daarnaast legt het Hof enkele voorwaarden op met betrekking tot deze regeling. Het moet namelijk ook duidelijke en nauwkeurige regels bevatten die aangeven wanneer en hoe de aanbieders van elektronische communicatiediensten aan de bevoegde nationale autoriteiten toegang tot die gegevens moeten verlenen.[125] Het Hof oordeelde ook dat de nationale wetgeving de materiële en procedurele voorwaarden voor toegang moet vaststellen op basis van objectieve criteria.[126] In dit verband kan in beginsel voor het doel van bestrijding van criminaliteit slechts toegang worden verleend tot de gegevens van personen die ervan worden verdacht een ernstig misdrijf te plannen, te plegen of te hebben gepleegd of op de een of andere wijze betrokken te zijn bij een dergelijk misdrijf.[127] Het Hof aanvaardt evenwel dat, bij wijze van uitzondering, toegang tot de gegevens van anderen zou worden verleend wanneer bijvoorbeeld vitale nationale belangen worden bedreigd door terroristische activiteiten. Dit geldt voor zover er op grond van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot de bestrijding van dergelijke activiteiten zouden kunnen leveren.[128]

[120] Tele 2 Watson, overw. 108.; C. FORGET, "L'obligation de conservation des "métadonnées": la fin d'une longue saga juridique?", *Journal des Tribunaux* 2017, (233) 238.
[121] Tele 2 Watson, overw. 109.; I. CAMERON, "Balancing data protection and law enforcement needs: Tele2 Sverige and Watson", *CML Rev.* 2017, (1467) 1479.
[122] Tele 2 Watson, overw. 110.; D. BIJNENS, "De wetgeving inzake dataretentie: *the saga continues…*" (noot onder HvJ 21 december 2018, gevoegde zaken nrs. C-203/15 en C-698/15, ECLI:EU:C:2016:970, *Tele2 Sverige AB* en *Secretary of State for the Home Department*), *TBP* 2017, (525) 526.
[123] Tele 2 Watson, overw. 111.; C. FORGET, "L'obligation de conservation des "métadonnées": la fin d'une longue saga juridique?", *Journal des Tribunaux* 2017, (233) 238.
[124] Tele 2 Watson, overw. 115.
[125] Telet 2 Watson, overw. 117.
[126] Tele 2 Watson, overw. 118-119.
[127] Tele 2 Watson, overw. 119
[128] *Ibid.*

Om te waarborgen dat deze voorwaarden in de praktijk worden gerespecteerd, stelt het Hof dat de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens in beginsel aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit wordt onderworpen.[129] Een uitzondering wordt voorzien voor de gevallen van naar behoren gerechtvaardigde spoedeisendheid.[130] Deze bevoegde nationale autoriteiten moeten ook de personen op wie de toegang tot de gegevens betrekking heeft, volgens de toepasselijke nationale procedures in kennis stellen, zodra deze kennisgeving het onderzoek niet langer in gevaar brengt. Het Hof benadrukte dat deze kennisgeving noodzakelijk is om deze personen in staat te stellen hun recht op een rechtsmiddel krachtens de e-Privacy Richtlijn en het EU-recht inzake gegevensbescherming uit te oefenen.[131]

Wat de beveiliging van de gegevens betreft, oordeelde het Hof dat artikel 15, lid 1 van de e-Privacy Richtlijn de lidstaten niet toestaat af te wijken van de bepalingen die de aanbieders verplichten passende technische en organisatorische maatregelen te nemen om een doeltreffende bescherming van de bewaarde gegevens te waarborgen.[132] Het Hof was van oordeel dat een bijzonder hoog niveau van gegevensbeveiliging passend was gezien de hoeveelheid en de aard van de bewaarde gegevens en het risicovolle karakter van deze operatie. Het oordeelde daarom dat de nationale wetgeving moet bepalen dat de gegevens binnen de EU worden bewaard en dat de gegevens aan het einde van de bewaringstermijn onomkeerbaar worden vernietigd.[133] De lidstaten moeten er ook voor zorgen dat een onafhankelijke autoriteit de naleving van het EU-recht controleert, aangezien een dergelijke onafhankelijke controle op de naleving van het gegevensbeschermingsrecht een essentieel element is van het in artikel 8, lid 3, van het EU-Handvest neergelegde recht op gegevensbescherming. Het Hof benadrukte het verband tussen een dergelijk onafhankelijk toezicht en de beschikbaarheid van een rechtsmiddel voor betrokkenen.[134] Het Hof concludeerde dan ook dat een nationale regeling die niet aan deze voorwaarden voldoet, uitgesloten is op grond van artikel 15, lid 1, gelezen in het licht van het EU-Handvest.[135] Het stond echter aan de betrokken nationale rechter om te onderzoeken of in het onderhavige geval aan die voorwaarden was voldaan.[136]

40. Wat ten slotte de vraag van de Britse Court of Appeal betreft over het verband tussen het recht op gegevensbescherming en privacy in het EU-Handvest en artikel 8 EVRM, oordeelde het Hof dat het antwoord op deze vraag niet van invloed is op de uitlegging van de e-Privacy Richtlijn en dus in deze procedure geen rol speelt.[137] Het herinnerde aan zijn vaste rechtspraak dat de prejudiciële procedure dient om geschillen van Unierecht daadwerkelijk op te lossen en niet om

[129] *Ibid*, overw. 120.
[130] *Ibid.*
[131] *Ibid*, overw. 121.
[132] Tele 2 Watson, overw. 122.; zie ook art. 4, lid 1 en art. 4 lid 1 *bis* e-Privacy Richtlijn.
[133] Tele 2 Watson, overw. 122.; T. VAN CANNEYT, A. BERTRAND, S. CROUZET en L. VANDERDONCKT, "Data Protection: CJEU case law review 1995-2020, *Computerrecht* 2021, (78) 138.
[134] Tele 2 Watson, overw. 123.; I. CAMERON, "Balancing data protection and law enforcement needs: Tele2 Sverige and Watson", *CML Rev.* 2017, (1467), 1480.
[135] Tele 2 Watson, overw. 125.; M. PANZAVOLTA, S. ROYER en H. SEVERIJNS, "Algemene dataretentie: ten minste houdbaar tot…?", *T. Strafr.* 2018, (3) 10.
[136] Tele 2 Watson, overw. 124.
[137] Tele 2 Watson, overw. 131.

advies te geven of hypothetische vragen te beantwoorden.[138] Het benadrukte dat het EVRM geen formeel onderdeel van het EU-recht vormt. Het merkte evenwel op dat artikel 52, lid 3 van het EU-Handvest tot doel heeft de samenhang tussen het EU-Handvest en het EVRM te waarborgen zonder afbreuk te doen aan de autonomie van het EU-recht. Het EU-recht staat er derhalve niet aan in de weg dat het een ruimere bescherming biedt dan het EVRM. Het Hof voegde daaraan toe dat artikel 8 van het EU-Handvest een grondrecht betreft dat verschilt van het in artikel 7 neergelegde grondrecht, dat geen equivalent heeft in het EVRM. Hoewel het Hof dus geen antwoord gaf op de vraag welk recht een ruimere bescherming biedt, bevestigde het wel het onderscheid tussen beide rechten.

41. **CONCLUSIE –** Dit arrest vormt de blauwdruk voor de toetsing van nationale maatregelen aan het EU-recht. Zoals hierboven is uiteengezet, onderzocht het Hof eerst of de bepalingen die de aanbieders verplichten tot het bewaren van gegevens, in overeenstemming zijn met het Unierecht. Ten tweede onderzocht het Hof of de bepalingen die de bevoegde nationale autoriteiten toegang verlenen tot die bewaarde gegevens, in overeenstemming zijn met de bepalingen van het Unierecht.

Met betrekking tot de verplichting tot het bewaren, oordeelde het Hof dus dat nationale wetgeving die voorziet in een **algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens,** waarbij:

- geen enkel verband tussen de bewaarde gegevens en een bedreiging van de openbare veiligheid bestaat;
- noch beperkt is tot gegevens binnen een bepaalde periode en/of een bepaald gebied en/of een kring van personen die op een of andere wijze betrokken kunnen zijn bij een ernstig strafbaar feit, of op personen van wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij de bestrijding van criminaliteit;

de grenzen van het strikt noodzakelijke overschrijden en niet kan worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is.

Daarentegen is een **preventieve gerichte bewaring van verkeersgegevens en locatiegegevens** ter bestrijding van zware criminaliteit wel toegelaten, op voorwaarde dat de bewaring van die gegevens, wat de categorieën van te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaren betreft, tot het strikt noodzakelijke wordt beperkt. Om hieraan te voldoen, moet de regeling:

- Duidelijke en nauwkeurige regels voor de draagwijdte en de toepassing van een dergelijke maatregel van bewaring van gegevens bevatten;
- Een minimum aan eisen stellen, zodat er voldoende garanties bestaan dat persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik;

[138] Tele 2 Watson, overw. 130.

- Aangeven in welke omstandigheden en onder welke voorwaarden een maatregel van bewaring van gegevens preventief kan worden genomen.
- Voldoen aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel.
- Gebaseerd zijn op objectieve elementen waarmee kan worden gemikt op een groep mensen wier gegevens, althans indirect, een band met handelingen van zware criminaliteit aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedrafen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de opennbare veiligheid kan worden voorkomen.
    - Een dergelijke afbakening kan aan de hand van een geografisch criterium worden verricht wanneer de bevoegde nationale autoriteiten op basis van objectieve elementen van mening zijn dat er in een of meer geografische gebieden een hoog risico bestaat dat dergelijke handelingen worden voorbereid of gepleegd.

Met betrekking tot de **toegang van bevoegde nationale tot de bewaarde verkeers- en locatiegegevens,** heeft het Hof erop gewezen dat alleen de bestrijding van zware criminaliteit een dergelijke toegang tot bewaarde gegevens kan rechtvaardigen. Daarnaast legt het Hof een aantal strikte voorwaarden op. De regeling moet:

- Duidelijke en nauwkeurige materiële en procedurele voorwaarden vaststellen voor de toegang tot de bewaarde gegevens.

- Duidelijke en nauwkeurige regels bevatten die aangeven wanneer en hoe de aanbieders van elektronische communicatiediensten aan de bevoegde nationale autoriteiten toegang tot die gegevens moeten verlenen.
    - Voor het doel van bestrijding van criminaliteit kan in beginsel slechts toegang worden verleend tot de gegevens van personen die ervan worden verdacht een ernstig misdrijf te plannen, te plegen of te hebben gepleegd of op de een of andere wijze betrokken te zijn bij een dergelijk misdrijf.
    - Een uitzondering is mogelijk wanneer vitale nationale belangen worden bedreigd door terroristische activiteiten, voor zover er op grond van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot de bestrijding van dergelijke activiteiten zouden kunnen leveren.
- Voorzien in een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit.
- Voorzien in een kennisgeving zodra deze kennisgeving het onderzoek niet langer in gevaar brengt.

3.3.2. C-207/16 – Ministerio Fiscal

42. **FEITEN –** De verwijzing vond plaats in het kader van een politieonderzoek naar de diefstal van een portefeuille en een mobiele telefoon. De Spaanse politie verzocht de onderzoeksrechter om toegang tot de gegevens ter identificatie van de gebruikers van telefoonnummers die met de gestolen telefoon zijn geactiveerd gedurende een periode van twaalf dagen vanaf de datum van de diefstal.[139] De onderzoeksrechter heeft dit verzoek afgewezen, onder meer omdat de feiten die aanleiding hebben gegeven tot het strafrechtelijk onderzoek geen "ernstig" misdrijf vormen.[140] Een ernstig misdrijf naar Spaans recht is een misdrijf waarop een gevangenisstraf van meer dan vijf jaar staat. De toegang tot deze gegevens is alleen mogelijk voor deze categorie van misdrijven.[141] Het Ministerio Fiscal (het Spaanse Openbaar Ministerie) is tegen deze beslissing in beroep gegaan bij de Audiencia Provincial de Tarragona (provinciale rechtbank van Tarragona, Spanje).[142] De Audiencia Provincial de Tarragona verzocht het Hof van Justitie derhalve om richtsnoeren voor de vaststelling van de drempel van de ernst van de strafbare feiten waarboven een inmenging in de grondrechten, zoals de toegang van de bevoegde nationale autoriteiten tot de door de aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens, gerechtvaardigd kan zijn.[143]

43. **ANALYSE VAN HET HOF –** Het Hof ging vooreerst zijn bevoegdheid na om kennis te nemen van de prejudiciële vragen. Zowel de Spaanse als de Britse regering betoogden dat het Hof niet bevoegd was, omdat de zaak betrekking had op een activiteit van de staat op strafrechtelijk gebied, en dus buiten de werkingssfeer van de e-Privacy Richtlijn viel krachtens de uitzondering in artikel 1, lid 3 van de e-Privacy Richtlijn. Het Hof verwees echter naar zijn eerdere arresten *Digital Rights Ireland* en *Tele2 Watson* waarin het oordeelde dat wettelijke maatregelen die op basis van artikel 15, lid 1 van de e-Privacy Richtlijn afwijken, toch binnen de werkingssfeer ervan vallen, zelfs indien de maatregelen doelstellingen nastreven die de bij artikel 1, lid 3, van de e-Privacy Richtlijn uitgesloten gebieden grotendeels overlappen.[144] Het Hof verduidelijkte dat artikel 15, lid 1, van de e-Privacy Richtlijn gelezen in samenhang met artikel 3 van de e-Privacy Richtlijn, aldus moet worden uitgelegd dat binnen de werkingssfeer van deze richtlijn niet alleen wettelijke maatregelen vallen die aanbieders van elektronische-communicatiediensten de verplichting opleggen om verkeers- en locatiegegevens te bewaren, maar ook wettelijke maatregelen inzake de toegang van nationale autoriteiten tot door die aanbieders bewaarde gegevens.[145] Vervolgens voerde de Spaanse regering aan dat het toegangsverzoek enkel betrekking had op de telefoonnummers die overeenstemmen het IMEI-nummer van de gestolen mobiele telefoon geactiveerde simkaarten en de civiele-identificatiegegevens van die kaarten, waardoor het geen verkeers- en locatiegegevens waren. Op deze manier zou het toegangsverzoek buiten het toepassingsgebied vallen van de e-Privacy Richtlijn. Het Hof oordeelt

[139] Ministerio Fiscal, overw. 20.
[140] Ministerio Fiscal, overw. 21.
[141] *Ibid.*
[142] Ministerio Fiscal, overw. 22.
[143] Ministerio Fiscal, overw. 26.
[144] Ministerio Fiscal, overw. 34.; C. DOCKSEY, "Ministerio Fiscal: Holding the line on ePrivacy", *Maastricht Journal of European and Comparative Law* 2019, (585) 588.
[145] Ministerio Fiscal, overw. 35.; A. CAIOLA, "À la recherche de la justice pondération entre ingérence dans la vie privée et nécessité de lutte contra la criminalité, *RAE* 2018, (719) 721.

echter, in navolging van de advocaat-generaal in punt 54 van zijn conclusie, dat de e-privacyrichtlijn van toepassing is op elke verwerking van persoonsgegevens in verband met de levering van elektronische communicatiediensten. Zij is niet beperkt tot verkeersgegevens betreffende daadwerkelijk verrichte communicaties en tot de locatiegegevens van de gestolen mobiele telefoon. Bijgevolg vallen gegevens die uitsluitend betrekking hebben op de identiteit van eigenaars of gebruikers van simkaarten, de zogenaamde "abonneegegevens", binnen de werkingssfeer van de e-Privacy Richtlijn. Ten slotte verwierp het Hof de ingeroepen excepties van niet-ontvankelijkheid van de prejudiciële vragen.[146]

44. Vervolgens zet het Hof zijn analyse verder ten gronde. De twee prejudiciële vragen worden door het Hof samen onderzocht en het herformuleert deze, zoals voorgesteld door de advocaat-generaal. De vraag luidt of art. 15 lid 1 van de e-Privacy Richtlijn in samenhang gelezen met de artikelen 7 en 8 van het EU-Handvest, zo moet worden uitgelegd dat de toegang van de overheidsinstanties tot de identificatiegegevens van de houders met een gestolen mobiele telefoon geactiveerde simkaarten een zodanig ernstige inmenging in de in het Handvest neergelegde fundamentele rechten inzake de persoonlijke levenssfeer en de gegevensbescherming vormt, dat de toegang zou moeten worden beperkt tot de bestrijding van zware criminaliteit en zo ja, aan de hand van welke criteria de ernst van het betrokken delict moet worden beoordeeld.[147]

Ten eerste stelt het Hof dat de toegang van nationale autoriteiten tot gegevens die door aanbieders van elektronische communicatiediensten worden bewaard, een inmenging vormt in de in het EU-Handvest neergelegde grondrechten van eerbiediging van het privéleven en bescherming van persoonsgegevens, ongeacht of die inmenging "ernstig" is.[148] Vervolgens merkt het Hof op dat de lijst van doelstellingen in de zin van artikel 15 van de e-Privacy Richtlijn limitatief is en dat de behoefte van de autoriteiten aan toegang daadwerkelijk aan een van deze doelstellingen moet beantwoorden.[149] In dit opzicht beperkt artikel 15 van de e-Privacy Richtlijn de toegang echter niet tot de bestrijding van zware criminaliteit. Het verwijst naar strafbare feiten in het algemeen. De verwijzing naar "ernstig" komt uit de rechtspraak van het Hof waarin het ging om situaties waarin sprake was van een ernstige inmenging in het recht op eerbiediging van het privéleven. Wanneer de inmenging die deze toegang met zich brengt daarentegen niet ernstig is, kan deze worden gerechtvaardigd door het doel om "strafbare feiten" in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen.[150] Vervolgens herdefinieerde het Hof het voorwerp van zijn overwegingen tot de vraag of de inmenging in casu "ernstig" was.[151] Aangezien de gevraagde gegevens slechts betrekking hadden op een korte periode en niet konden worden vergeleken met andere gegevens, konden geen precieze conclusies over het privéleven van de betrokken personen worden getrokken.[152] Derhalve was er geen sprake van

[146] Ministerio Fiscal, overw. 45.
[147] Ministerio Fiscal, overw. 45.
[148] Ministerio Fiscal, overw. 51.
[149] Ministerio Fiscal, overw.52; A. CAIOLA, "À la recherche de la justice pondération entre ingérence dans la vie privée et nécessité de lutte contra la criminalité, *RAE* 2018, (719) 725.
[150] Ministerio Fiscal, overw. 57.
[151] Ministerio Fiscal, overw. 58 – 62.; C. VAN DE HEYNING, "Het moeilijke evenwicht tussen privacy & veiligheid: De impact van het debat over bewaren van communicatiegegevens", *Radices* 2022, (132) 141.
[152] Ministerio Fiscal, overw. 59-60.

een ernstige inmenging in het recht op privéleven van de betrokkenen en kon de toegang tot dergelijke gegevens worden gerechtvaardigd.[153]

45. **CONCLUSIE –** Het Hof neemt afstand van de moeilijke vraag door zijn herformulering van de prejudiciële vraag van de verwijzende rechter. Daarmee vermeed het Hof niet alleen de definiëring van wat "ernstige criminaliteit" is, maar ook de vraag of "ernstige criminaliteit" een autonoom EU-begrip is. Dit ligt in lijn met het advies van de advocaat-generaal. De advocaat-generaal ontraadde de vaststelling van een definitie van een "ernstig strafbaar feit" in de zin van *Digital Rights Ireland* en *Tele2 Watson*. Hij betoogde dat het begrip "ernstig misdrijf" "geen autonoom Unierechtelijk begrip is waarvan de inhoud door het Hof moet worden bepaald", maar veeleer afhankelijk is van de rechtsorde van elke lidstaat,[154] met dien verstande dat de afwijking van artikel 15, lid 1, van de e-Privacy Richtlijn moet worden uitgelegd in overeenstemming met de door het Handvest gewaarborgde grondrechten.[155] Het komt toe aan de lidstaten om te bepalen wat een 'ernstig misdrijf' uitmaakt, zolang dit gebaseerd is op een objectieve verantwoording rekening houdende met de ernst van de beperking op de fundamentele rechten en de ernst van het misdrijf. De drempel van "ernstig misdrijf" wordt bepaald door de ernst van de beperking van de bescherming van persoonsgegevens en de persoonlijke levenssfeer af te wegen tegen de ernst van de feiten. Interessant aan dit arrest is dat het Hof van Justitie in zijn eerdere arrest *Tele2 Watson* had geoordeeld dat de toegang tot de bewaarde gegevens beperkt is tot gevallen waarin sprake is van ernstige criminaliteit. Om de twee arresten met elkaar in overeenstemming te brengen, legt het Hof uit dat dit komt doordat het met de toegang nagestreefde doel evenredig moet zijn aan de ernst van de inbreuk op de grondrechten die de toegang met zich brengt. De zaak *Tele2 Watson* betreft de toegang tot bewaarde gegevens die, in hun geheel beschouwd, nauwkeurige conclusies over het privéleven van de betrokken personen mogelijk maken. Een dergelijke toegang vormt een ernstige inbreuk op de grondrechten en kan alleen worden gerechtvaardigd door het doel om zware criminaliteit te bestrijden. Indien de toegang tot bewaarde gegevens echter een niet-ernstige inmenging is, zoals in casu de toegang tot de identiteit van de abonnee, kan de toegang worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van "strafbare feiten" in het algemeen.

[153] Ministerio Fiscal, overw. 62.
[154] Concl. A-G H. SAUGMANDSGAARD ØE, ECLI:EU:C:2018:300, bij HvJ (Grote Kamer) 2 oktober 2018, nr. C-207/16, ECLI:EU:C:2018:788, Ministerio Fiscal, overw. 93-99.
[155] *Ibid*, 100-101.

3.3.3. C-511/18 – La Quadrature du Net en C-623/17 – Privacy International

46. **FEITEN –** Verschillende rechtbanken in Groot-Brittannië, Frankrijk en België hebben het Hof van Justitie de vraag gesteld of artikel 15, lid 1 van de e-Privacy Richtlijn zo moet worden geïnterpreteerd dat het zich verzet tegen nationale regelgeving die elektronische communicatiediensten verplicht om verkeers- en locatiegegevens algemeen en ongedifferentieerd te bewaren en te delen met de bevoegde autoriteiten, in het belang van nationale veiligheid.[156] Het Hof heeft over deze vraag uitspraak gedaan in de arresten *La Quadrature du Net* en *Privacy International* op 6 oktober 2020. De Britse zaak wordt behandeld in het arrest *Privacy International*, terwijl de Franse en Belgische zaken gezamenlijk worden behandeld in *La Quadrature du Net*. De twee zaken staan los van elkaar, met verschillende uitkomsten, maar de kwesties zijn zo nauw met elkaar verbonden dat het verstandig is ze samen te behandelen.

Tegen de achtergrond van de "Snowden-onthullingen" werd de rechtmatigheid van het verzamelen en gebruiken van communicatiegegevens in bulk door de veiligheids- en inlichtingendiensten van het Verenigd Koninkrijk betwist door de NGO Privacy International.[157] De wet bepaalde dat de verantwoordelijke minister telecommunicatieaanbieders kan opdragen alle of een deel van de gegevens waarover zij beschikken over te dragen aan de veiligheids- en inlichtingendiensten. Deze "bulk communicatiegegevens" worden vervolgens samengevoegd met andere "bulk" datasets en geanalyseerd.[158] Hoewel de Investigatory Powers Act 2016 het systeem van regulering en de onafhankelijke controles op de manier waarop de veiligheids- en inlichtingendiensten deze gegevens verwerven en gebruiken verbetert, bestaat er geen twijfel over dat dit systeem ten tijde van de zaak gepaard gaat met de "algemene en ongedifferentieerde overdracht van gegevens".[159] De "Investigatory Powers Tribunal" stelde het Hof van Justitie de prejudiciële vraag of het bestaan van dergelijke praktijken binnen de werkingssfeer van het Unierecht en van de e-Privacy Richtlijn valt en, zo ja, of het Unierecht zich verzet tegen een nationale regeling op grond waarvan overheidsinstanties aanbieders van elektronische communicatiediensten kunnen verplichten tot het "algemeen en ongedifferentieerd" doorgeven van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten ter waarborging van de nationale veiligheid.[160]

Bij beroepen van 30 november 2015 en 16 maart 2016 hebben verschillende belangengroepen en non-profitorganisaties bij de Franse Conseil d'État beroepen ingesteld tot nietigverklaring van de decreten op grond waarvan exploitanten van elektronische communicatie en technische dienstverleners "op hun netwerken geautomatiseerde

[156] La Quadrature du Net, overw. 68, 73 en 79.; Privacy International, overw. 29.; N.A. SMUHA, (noot onder HvJ (grote kamer) 6 oktober 2020, C-623/17 (Privacy International) en gevoegde zaken C-511/18, C-512/18 en C-520/18 (La Quadrature du Net e.a.), *TBP* 2022, (540) 541.
[157] J. BERGHOLM, "The Data Retention Saga Continued - from *Tele2 Sverige* to *Privacy International* and *La Quadrature du Net"*, *JFT* 2021, (111) 111.
[158] I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1438.
[159] *Ibid.*
[160] Privacy International, overw. 29

gegevensverwerkingspraktijken moeten toepassen die erop gericht zijn (...) verbanden op te sporen die een terroristische dreiging kunnen vormen".[161] Verzoekers stelden dat de decreten in strijd waren met de Franse grondwet, het EVRM en de richtlijnen 2000/31 en 2002/58 (betreffende de bescherming van persoonsgegevens en de persoonlijke levenssfeer).[162] De Conseil d'État besloot de procedure te schorsen en drie prejudiciële vragen voor te leggen.[163] Ten eerste, of het bij de regeling ingevoerde systeem, zoals hierboven beschreven, kan worden gerechtvaardigd op grond van het feit dat het EU-Handvest van de grondrechten voorziet in een recht op veiligheid, en het feit dat volgens artikel 4, lid 2 VEU alleen de lidstaten verantwoordelijk zijn voor de nationale veiligheid. Ten tweede, of de e-Privacy Richtlijn, gelezen in het licht van het EU-Handvest, wettelijke maatregelen toestaat die de realtimeverzameling van verkeers- en locatiegegevens van bepaalde personen mogelijk maken, maar die aanbieders van een elektronische-communicatiedienst niet verplichten om hun gegevens in het algemeen te bewaren. Ten derde, of het noodzakelijk is om personen die door dergelijke maatregelen voor de verzameling van metadata worden getroffen, te informeren.

Volgens de Belgische telecomwet, die in 2016 is gewijzigd ingevolge het *Digital Rights Ireland*-arrest, geldt voor alle aanbieders van telecommunicatiediensten een algemene bewaarplicht van verkeers- en locatiegegevens gedurende een periode van 12 maanden.[164] Deze gegevens moeten op verzoek beschikbaar worden gesteld, met inachtneming van de beperkingen en procedures die in afzonderlijke wetten zijn vastgelegd, voor strafrechtelijk onderzoek, voor lokalisatiedoeleinden in noodsituaties en voor de inlichtingendiensten.[165] Twee advocatenverenigingen en een aantal mensenrechtengroeperingen hebben bij het Belgische Grondwettelijk Hof beroep tot nietigverklaring van de wet van 2016 ingesteld omdat deze in strijd zou zijn met de Belgische Grondwet, het EVRM en het EU-Handvest.[166] Het Belgische Grondwettelijk Hof schorste deze procedures en vroeg om een prejudiciële beslissing waarin drie vragen werden gesteld.[167] De eerste vraag was vergelijkbaar met de eerste vraag van de Franse Conseil d'état. De tweede vraag was of een dergelijke algemene bewaarplicht kan worden gerechtvaardigd om te voldoen aan een positieve verplichting van de Staat om te voorzien in een rechtskader dat een doeltreffend onderzoek naar misdrijven, zoals seksueel misbruik van een minderjarige, mogelijk maakt. De derde vraag was of, indien algemene bewaring niet toelaatbaar zou zijn, het niettemin toelaatbaar zou kunnen zijn om op tijdelijke basis de gevolgen te handhaven om rechtsonzekerheid te voorkomen en ervoor te zorgen dat de eerder verzamelde en bewaarde gegevens verder kunnen worden gebruikt voor de door de wet nagestreefde doelstellingen.

[161] S. ESKENS, "The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature du Net and Others and Privacy International", *EDPL* 2022, 144-145.
[162] *Ibid.*
[163] La Quadrature du Net, overw. 73.
[164] J. BERGHOLM, "The Data Retention Saga Continued - from *Tele2 Sverige* to *Privacy International* and *La Quadrature du Net"*, *JFT* 2021, (111) 118.
[165] La Quadrature du Net, overw. 77.
[166] I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1441.
[167] La Quadrature du Net, overw. 79.

47. **ANALYSE VAN HET HOF –** Opnieuw was het aan het Hof om te oordelen of de nationale maatregelen in eerste instantie binnen de werkingssfeer van de e-Privacy Richtlijn vielen.[168] Het Hof van Justitie herhaalde zijn benadering in *Tele 2 Watson,* waarin werd vastgesteld dat een redenering volgens welke de in artikel 15, lid 1, ervan bedoelde wettelijke maatregelen van de werkingssfeer van de richtlijn zijn uitgesloten omdat de doelstellingen die dergelijke maatregelen moeten nastreven, grotendeels overeenstemmen met de doelstellingen van de in artikel 1, lid 3, e-Privacy Richtlijn bedoelde activiteiten, artikel 15, lid 1, elk nuttig effect ontnemen.[169] Het Hof stelt verder dat artikel 4, lid 2, VEU kan niet afdoen aan deze conclusie.[170] Het enkele feit dat een lidstaat een maatregel heeft genomen ter bescherming van de nationale veiligheid, volstaat niet om buiten de toepassing van het Unierecht buiten te vallen.[171] Bijgevolg kan een nationale regeling die elektronische communicatiediensten verplicht algemeen en ongedifferentieerd verkeers- en locatiegegevens door te geven aan veiligheids- en inlichtingendiensten ter bescherming van de nationale veiligheid *(Privacy International)* vallen binnen de werkingssfeer van de e-Privacy Richtlijn.[172] Dit geldt ook voor een nationale regeling die, ten behoeve van 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 oplegt.[173]

48. Vervolgens gaat het Hof verder met de uitlegging van artikel 15, lid 1 van de e-Privacy Richtlijn. Belangrijk is dat het Hof opmerkt dat de bewaring van verkeers- en locatiegegevens voor politiële doeleinden op zichzelf afbreuk kan doen aan het in artikel 7 van het EU-Handvest verankerde recht op eerbiediging van communicatie en de gebruikers van elektronischecommunicatiemiddelen kan ontmoedigen om hun door artikel 11 van het EU-Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen.[174] Deze rechten hebben echter geen absolute gelding, maar moeten worden beschouwd in relatie tot hun functie in de samenleving.[175] Er moet daarnaast ook rekening worden gehouden met het belang van de doelstellingen van bescherming van de nationale veiligheid en bestrijding van zware criminaliteit als bijdrage aan de bescherming van de rechten en vrijheden van anderen.[176] Meer bepaald volgt uit de rechtspraak van het Hof dat de beperkingen die de lidstaten invoeren, moeten worden beoordeeld door de ernst te meten van de inmenging die een dergelijke beperking met zich meebrengt en door na te gaan of het belang van de met die beperking nagestreefde doelstelling

[168] I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1446-1447.
[169] La Quadrature du Net, overw. 97.
[170] La Quadrature du Net, overw. 99.
[171]La Quadrature du Net, overw. 99.; I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1447.; N.A. SMUHA, (noot onder HvJ (grote kamer) 6 oktober 2020, C-623/17 (Privacy International) en gevoegde zaken C-511/18, C-512/18 en C-520/18 (La Quadrature du Net e.a.), *TBP* 2022, (540) 541.
[172] Privacy International, overw. 49.
[173] La Quadrature du Net, overw. 104.; X. TRACOL, "The two judgements of the European Court of Justice in the court cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is trying hard to square the circle of data retention, *COMPUTER LAW & SECURITY REVIEW* 2021*,* (1) 4.
[174] La Quadrature du net, overw. 118.
[175] La Quadrature du net, overw. 120.; X. TRACOL, "The two judgements of the European Court of Justice in the court cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is trying hard to square the circle of data retention, *COMPUTER LAW & SECURITY REVIEW* 2021*,* (1) 5.
[176] La Quadrature du Net, overw. 122.

van algemeen belang in verhouding staat tot die ernst.[177] Daarbij moesten drie elementen worden onderzocht: de rechtsgrondslag, de eerbiediging van het wezen van het recht en de evenredigheid (beperkingen zijn noodzakelijk en beantwoorden daadwerkelijk aan doelstellingen van algemeen belang).[178]

49. Hierna ging het Hof in op de kwestie van **de wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bescherming van de nationale veiligheid.** Het Hof heeft zich in zijn arresten nog niet specifiek gebogen over de doelstelling van bescherming van de nationale veiligheid. In dit verband stelt het Hof dat nationale veiligheid volgens artikel 4, lid 2 VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten.[179] Het Hof gaat verder en merkt op dat het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, verder gaat dan dat van de andere in artikel 15, lid 1 van de e-Privacy Richtlijn genoemde doelstellingen. De doelstelling van bescherming van de nationale veiligheid kan derhalve maatregelen rechtvaardigen die ernstigere inbreuken op de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd.[180] Het bevel om preventief de gegevens te bewaren van alle gebruikers van elektronischecommunicatiemiddelen, mag echter slechts worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk.[181] Het opgelegde bevel tot bewaring van die gegevens kan echter worden verlengd wegens het voortduren van een dergelijke bedreiging, maar dit neemt niet weg dat elk bevel slechts mag worden gegeven voor een voorzienbare periode.[182] Daartoe is het van wezenlijk belang dat een beslissing waarbij aan aanbieders van elektronischecommunicatiediensten een bevel tot een dergelijke gegevensbewaring 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.[183]

[177] La Quadrature du Net, overw. 133.
[178] I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1448.
[179] La Quadrature du Net, overw. 135.; I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1448.
[180] La Quadrature du Net, overw. 137.; X. TRACOL, "The two judgements of the European Court of Justice in the court cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is trying hard to square the circle of data retention, *COMPUTER LAW & SECURITY REVIEW* 2021*,* (1) 6.
[181] La Quadrature du Net, overw. 138.; C. DE TERWAGNE, "L'illégalité nuancée de la surveillance numérique: la réponse des juridictions belge et française à l'arrêt *La Quadrature du Net* de la Cour de justice de L'Union européenne, *RevTrimDrH* 2022, (3) 13.
[182] *Ibid*.
[183] La Quadrature du Net, overw. 139.

50. Daarentegen stelde het Hof dat een nationale regeling die voorziet in de **algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit,** verder gaat dan strikt noodzakelijk is en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is.[184] Zoals het Hof reeds heeft geoordeeld in *Tele 2 Watson*, beperkt een dergelijke regeling met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het bestrijden van zware criminaliteit.[185] Een gerichte bewaring op basis van de eisen gesteld in *Tele 2 Watson* is wel toegelaten. Hierbij verduidelijkt het Hof wat het bedoelde met de verzameling van verkeers- en locatiegegevens op basis van een geografisch criterium. Volgens het Hof gaat het om gebieden "met een hoge incidentie van ernstige criminaliteit, plaatsen die bijzonder kwetsbaar zijn voor het plegen van ernstige strafbare feiten, zoals plaatsen of infrastructuren die regelmatig een zeer groot aantal bezoekers ontvangen, of strategische locaties, zoals luchthavens, stations of tolzones".[186]

51. **Vervolgens onderzoekt het Hof de wettelijke maatregelen die voorzien in de preventieve bewaring van IP-adressen en gegevens inzake de burgerlijke identiteit ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid**. Het Hof merkt op dat IP-adressen weliswaar behoren tot de verkeersgegevens, maar los van een bepaalde communicatie worden gegenereerd en hoofdzakelijk dienen om via de aanbieders van elektronischecommunicatiediensten de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd.[187] Voor zover bij e-mailverkeer en internettelefonie uitsluitend de IP-adressen van de bron van de communicatie en niet die van de ontvanger ervan worden bewaard, geven die adressen als zodanig geen enkele informatie prijs over de derden die in contact zijn geweest met de persoon die aan de basis ligt van de communicatie.[188] Deze categorie gegevens is dan ook van mindere gevoelige aard dan de andere verkeersgegevens. Aangezien IP-adressen echter ook kunnen worden gebruikt om de volledige online-activiteit van een internetgebruiker te volgen en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld.[189] De voor een dergelijke tracking noodzakelijke bewaring en analyse van IP-adressen vormen dan ook ernstige inmengingen in de door de artikelen 7 en 8 van het EU-Handvest gewaarborgde grondrechten van de internetgebruiker, die een ontmoedigend effect kunnen hebben.[190] Gelet op het feit dat die bewaring een ernstige inmenging inhoudt in de grondrechten die zijn verankerd in de artikelen 7

[184] La Quadrature du Net, overw. 141.
[185] La Quadrature du Net, overw. 144.
[186] La Quadrature du net, overw. 150.; I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1450.
[187] La Quadrature du net, overw. 152.
[188] *Ibid.*
[189] La Quadrature du net, overw 153.; I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1450.
[190] La Quadrature du net, overw 155.; X. TRACOL, "The two judgements of the European Court of Justice in the court cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is trying hard to square the circle of data retention, *COMPUTER LAW & SECURITY REVIEW* 2021*,* (1) 7.

en 8 van het EU-Handvest, kunnen enkel de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid, alsmede de bescherming van de nationale veiligheid, die inmenging rechtvaardigen.[191] Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk is gelet op het nagestreefde doel.[192] Tot slot moet een dergelijke maatregel voorzien in strikte voorwaarden en waarborgen met betrekking tot het gebruik van die gegevens, met name in de vorm van het in kaart brengen van de onlinecommunicatie en de online activiteiten van de betrokken personen.[193] Wat ten slotte de burgerlijke identiteitsgegevens betreft, moet worden opgemerkt dat met die gegevens alleen noch de datum, het tijdstip, de duur en de ontvangers van de communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Die gegevens verschaffen dus, afgezien van de contactgegevens van de betrokken gebruikers, zoals hun adres, geen informatie over wat die personen hebben gecommuniceerd en dus over hun privéleven. De inmenging die de bewaring van die gegevens met zich brengt, kan derhalve niet als „ernstig" worden aangemerkt. Het is met andere woorden een maatregel die als doelstelling het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid kan nastreven, zonder dat het daarbij hoeft te gaan om ernstige strafbare feiten of om ernstige bedreigingen en verstoringen van de openbare veiligheid.[194]

52. Het Hof boog zich ook over **wettelijke maatregelen die voorzien in de spoedbewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit.** Het Hof merkt op dat telecommunicatie-aanbieders de verkeers- en locatiegegevens na afloop van de bewaartermijn wissen of anonimiseren. Tijdens de bewaartermijn kunnen zich echter situaties voordoen waarin het noodzakelijk wordt die gegevens na afloop van die termijnen te bewaren om licht te werpen op ernstige strafbare feiten of handelingen die de nationale veiligheid schaden.[195] Verscheidene staten hebben daarom in hun wetgeving voorzien in de mogelijkheid om in specifieke gevallen een bevel tot langere bewaring te geven. Het kan daarbij gaan om personen of groepen waartegen vervolging wegens specifieke strafbare feiten is of wordt ingesteld, maar ook om personen die redelijkerwijs van criminele activiteiten worden verdacht en die derhalve in de toekomst kunnen worden vervolgd. Het Hof oordeelde dat dergelijke bevelen tot bewaring verenigbaar zijn met de e-Privacy Richtlijn, gelezen in het licht van het EU-Handvest, maar dat deze bevelen beperkt moeten blijven tot ernstige criminaliteit of de bescherming van de nationale veiligheid. Bovendien mag de bewaarplicht alleen betrekking hebben op de categorieën verkeers- en locatiegegevens die voor deze doeleinden objectief nuttig zijn.[196] De duur van de bewaring van die gegevens moet beperkt blijven tot het strikt

[191] *Ibid.*
[192] La Quadrature du Net, overw. 156.; X. TRACOL, "The two judgements of the European Court of Justice in the court cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is trying hard to square the circle of data retention, *COMPUTER LAW & SECURITY REVIEW* 2021*,* (1) 7.
[193] *Ibid*.
[194] La Quadrature du Net, overw. 159.
[195] La Quadrature du Net, overw. 162.
[196] I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1451.

noodzakelijke, hoewel die duur zo nodig kan worden verlengd.[197] De groep personen die het voorwerp van dergelijke bevelen tot bewaring kan zijn, zijn onder andere personen dan die welke redelijkerwijs van specifieke strafbare feiten worden verdacht: "mits die gegevens op basis van objectieve en niet-discriminerende factoren licht kunnen werpen op een dergelijk strafbaar feit of handelingen die de nationale veiligheid aantasten, zoals gegevens over het slachtoffer ervan, zijn of haar sociale of beroepskring, of zelfs bepaalde geografische gebieden, zoals de plaats waar het betrokken strafbare feit of de betrokken handeling die de nationale veiligheid aantast, is gepleegd of voorbereid".[198]

De tweede en de derde vraag in zaak C-511/18 hadden betrekking op twee verschillende Franse systemen voor onderzoek naar terrorisme die gebruik maken **geautomatiseerde analyse van verkeers- en locatiegegevens.** Het eerste systeem bevatte een verplichting voor alle aanbieders van elektronische communicatie om alle verkeers- en locatiegegevens volgens bepaalde algoritmen te filteren.[199] Het Hof stelde vast dat deze maatregel in kwestie een "algemene en ongedifferentieerde" draagwijdte had, aangezien het van toepassing was op alle personen die gebruikmaken van elektronischecommunicatiemiddelen.[200] Een dergelijke regeling vormt een bijzonder ernstige inbreuk in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, ongeacht het latere gebruik van die gegevens.[201] Tot slot kan zo'n regeling een ontmoedigend effect hebben op de uitoefening van de door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting. Het Hof vond echter dat dit deze maatregelen slechts aan het evenredigheidsvereiste kunnen voldoen in situaties waarin een lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en op voorwaarde dat de duur van die bewaring tot het strikt noodzakelijke wordt beperkt.[202] Het Hof verklaart dat, om in overeenstemming te zijn met het evenredigheidsbeginsel van wezenlijk belang is dat de beslissing waarbij de geautomatiseerde analyse wordt toegestaan, 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 zich een situatie voordoet die die maatregel rechtvaardigt, en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien. In dit verband dient te worden gepreciseerd dat de vooraf vastgestelde modellen en criteria waarop dit type gegevensverwerking is gebaseerd, ten eerste specifiek en betrouwbaar moeten zijn, zodat zij tot resultaten leiden waarmee die personen worden geïdentificeerd op wie een redelijk vermoeden van deelneming aan terrorisme kan rusten, en ten tweede niet mogen discrimineren.[203] Wat het non-discriminatievereiste betreft, merkt het Hof op dat het niet is toegestaan om bij het opstellen

[197] La Quadrature du Net, overw. 164.; X. TRACOL, "The two judgements of the European Court of Justice in the court cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is trying hard to square the circle of data retention, *COMPUTER LAW & SECURITY REVIEW* 2021*,* (1) 7.
[198] La Quadrature du Net, overw. 165.
[199] I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1452.
[200] *Ibid.*
[201] La Quadrature du Net, overw. 176.
[202] La Quadrature du Net, overw. 177.; DE TERWAGNE, "L'illégalité nuancée de la surveillance numérique: la réponse des juridictions belge et française à l'arrêt *La Quadrature du Net* de la Cour de justice de L'Union européenne, *RevTrimDrH* 2022, (3) 14.
[203] La Quadrature du Net, overw. 179.

van de modellen en criteria ter identificatie van terroristische dreigingen uit te gaan van "ras of etnische afkomst, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuiging, lidmaatschap van een vakvereniging, of informatie over iemands gezondheid of seksueel gedrag", zonder rekening te houden met het individuele gedrag van de betrokkene.[204] Bovendien preciseerde het Hof dat wanneer de zoekcriteria een positief resultaat opleveren, "alvorens een voor de betrokkenen nadelige individuele maatregel wordt genomen, zoals het achteraf in real time verzamelen van verkeers- en locatiegegevens", "een individueel heronderzoek met niet-geautomatiseerde middelen" moet plaatsvinden.[205] Er moet regelmatig worden nagegaan of de vooraf vastgestelde modellen en criteria en de gebruikte databanken betrouwbaar en actueel zijn.

Vervolgens gaat het Hof in op het tweede systeem, waarbij een individueel machtiging kan worden verleend voor in real time van verkeers- en locatiegegevens voor zover het gaat om "een persoon die eerder in verband is gebracht met een (terroristische) dreiging".[206] De gegevens waarop een dergelijke maatregel betrekking heeft, stellen de bevoegde nationale autoriteiten in staat om voor de duur van de machtiging continu en in real time in de gaten te houden met wie, met welke middelen en hoelang de betrokken personen communiceren, alsook waar zij verblijven en waarheen zij zich verplaatsen.[207] Ook lijkt uit die gegevens de aard van de online geraadpleegde informatie te kunnen worden afgeleid.[208] Het vormt volgens het Hof duidelijk een ernstige inbreuk op het recht op gegevensverwerking, op de persoonlijke levenssfeer en op de vrijheid van meningsuiting. Aangezien dergelijke gegevens dus als bijzonder gevoelig moeten worden beschouwd, dient de realtimetoegang van de bevoegde autoriteiten tot die gegevens te worden onderscheiden van de toegang daartoe die niet in real time plaatsvindt. De eerste soort toegang is ingrijpender omdat deze het mogelijk maakt om vrijwel alle gangen van de betrokken gebruikers na te gaan. Die inmenging gaat nog verder wanneer de opvraging in real time zich ook uitstrekt tot de verkeersgegevens van de betrokken personen. Het Hof maakt een onderscheid tussen "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 "andere personen van wie wordt aangenomen dat zij op enigerlei wijze in verband staan met terroristische activiteiten". Het Hof was van oordeel dat de eerstgenoemde categorie kan worden onderworpen aan een gecombineerde realtimeverzameling van verkeers- en locatiegegevens; de laatstgenoemde categorie alleen aan een niet-realtime-verzameling van verkeers- en locatiegegevens, en dan alleen "wanneer er objectieve aanwijzingen zijn waaruit kan worden afgeleid dat die gegevens in een concreet geval doeltreffend kunnen bijdragen tot de bestrijding van terrorisme".[209] Het Hof eiste dat in dit systeem soortgelijke waarborgen worden ingebouwd als in het eerste systeem, met de toevoeging dat de uitvoering van een maatregel die het verzamelen in real time toestaat, vooraf wordt getoetst door een rechter of door een

[204] La Quadrature du Net, overw. 181.
[205] La Quadrature du Net, overw. 182.; I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1453.
[206] La Quadrature du Net, overw. 183.
[207] La Quadrature du Net, overw. 184.
[208] *Ibid.*
[209] La Quadrature du Net, overw. 188.; I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1453.

onafhankelijk bestuursorgaan waarvan de beslissing bindend is en dat zich uitspreekt over de kern van de zaak, namelijk of het verzamelen van gegevens strikt noodzakelijk is.[210]

53. Met betrekking tot de **informatieverstrekking aan de personen van wie de gegevens zijn opgevraagd of geanalyseerd**, herhaalde het Hof dat kennisgeving aan personen die worden getroffen door eisen inzake bewaring van en toegang tot metadata noodzakelijk is om hen in staat te stellen hun rechten uit hoofde van het Handvest uit te oefenen.[211] Er bestond een kennisgevingsplicht voor personen die onderworpen zijn aan realtime verzameling van verkeers- en locatiegegevens, maar dat was niet het geval voor het bovengenoemde algoritmische systeem.[212] Het Hof overweegt dat wanneer de bevoegde autoriteit "de betrokkene identificeert om de hem betreffende gegevens grondiger te analyseren, deze persoon daarvan individueel in kennis moet worden gesteld.[213] Deze kennisgeving mag echter slechts plaatsvinden voor zover en zodra zij de taken waarmee deze autoriteiten zijn belast, niet meer in gevaar kan brengen.[214]

54. **CONCLUSIE –** *Privacy International* en *La Quadrature du Net* zijn mijlpaalarresten in de context van nationale veiligheid en terrorismebestrijding. Hoewel ze samen moeten worden behandeld, verschillen ze toch van elkaar. *Privacy International* zet de vaste verwerping door het Hof van algemene en ongedifferentieerde bewaring van gegevens voort, zelfs indien dit gebeurt met het oog op de nationale veiligheid. *La* Quadrature *du Net* markeert het begin van een meer genuanceerde benadering van surveillance die de deur opent voor zelfs massale bewaring van gegevens wanneer die nodig is voor terrorismebestrijding. Maatregelen voor gegevensbewaring lijken nu geleidelijk te worden toegestaan op basis van een reeks procedures, criteria en waarborgen waaronder zij moeten functioneren. Dit kan worden samengevat als volgt:

Algemene en ongedifferentieerde verzameling van verkeers- en locatiegegevens is mogelijk, indien:

- De doelstelling de bescherming is van de nationale veiligheid om ernstige bedreigingen voor de nationale veiligheid te voorkomen die "reëel en actueel of voorzienbaar zijn".
- Het bevel kan zonder onderscheid alle gebruikers van elektronische communicatie treffen, maar moet beperkt zijn in de tijd (hoewel verlenging mogelijk is).
- Het bevel tot bewaring moet worden onderworpen aan "effectieve toetsing, hetzij door een rechtbank, hetzij door een onafhankelijke administratieve instantie waarvan de beslissing bindend is", waarbij de toetsing tot doel heeft na te gaan of "een van deze situaties zich voordoet en of de voorwaarden en waarborgen die moeten worden gesteld, in acht worden genomen".

Gerichte bewaring van verkeers- en locatiegegevens is mogelijk, indien:

- De doelstelling het bestrijden van ernstige criminaliteit en/of het voorkomen van ernstige bedreigingen van de openbare veiligheid inhoudt.

[210] La Quadrature du Net, overw. 189.
[211] I. CAMERON, "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, (1443) 1453-1454.
[212] *Ibid.*
[213] La Quadrature du Net, overw.191.
[214] *Ibid.*

- De gerichte bewaring van verkeers- en locatiegegevens wordt beperkt, "op basis van objectieve en niet-discriminerende factoren". De beperkingen kunnen:
    - i) worden vastgesteld volgens de categorieën van betrokken personen op basis van objectief bewijsmateriaal dat het mogelijk maakt zich te richten op personen wier verkeers- en locatiegegevens waarschijnlijk een verband, althans een indirect verband, met ernstige strafbare feiten aan het licht zullen brengen; of
    - ii) aan de hand van een geografisch criterium dat is vastgesteld op basis van objectieve en niet-discriminerende factoren (gebieden kunnen plaatsen omvatten waar veel ernstige criminaliteit voorkomt, plaatsen die bijzonder kwetsbaar zijn voor het plegen van ernstige strafbare feiten, zoals plaatsen of infrastructuur die regelmatig een zeer groot aantal bezoekers ontvangen, of strategische locaties, zoals luchthavens, stations…).

- De duur niet langer is dan strikt noodzakelijk in het licht van het nagestreefde doel en de omstandigheden die deze rechtvaardigen, onverminderd de mogelijkheid om deze maatregelen te verlengen indien de bewaring noodzakelijk blijft.

De <u>preventieve bewaring van IP-adressen</u> is mogelijk, indien:

- De doelstelling de bestrijding van ernstige criminaliteit, de voorkoming van ernstige dreigingen voor de openbare veiligheid of de bescherming van de nationale veiligheid" inhoudt
- De bewaartermijn niet langer is dan strikt noodzakelijk is in het licht van het nagestreefde doel".
- De maatregel strikte voorwaarden en waarborgen vaststelt voor het gebruik van deze gegevens, met name via tracking, met betrekking tot de door de betrokken personen gedane handelingen en onlineactiviteiten.

De <u>preventieve bewaring van gegevens inzake de burgerlijke identiteit</u> is mogelijk, indien:

- Nationale maatregelen betreffende de verwerking van gegevens betreffende de burgerlijke identiteit, met inbegrip van het bewaren van en de toegang tot die gegevens uitsluitend gericht zijn op de identificatie van de betrokken gebruiker, en "zonder dat die gegevens in verband kunnen worden gebracht met informatie over de gedane mededelingen", kunnen worden gerechtvaardigd door het doel strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen. Dit is zelfs het geval wanneer de wetgeving geen specifieke termijn oplegt.

De <u>versnelde bewaring van verkeers- en locatiegegevens</u> is mogelijk, indien:

- Het doel van de maatregel de bestrijding van ernstige criminaliteit en *a fortiori* de bescherming van de nationale veiligheid uitmaakt
- Het bevel tot versnelde bewaring moet worden uitgevaardigd door de bevoegde autoriteit zoals bepaald in het recht van de lidstaat.
- Het bevel onderworpen is aan effectieve rechterlijke toetsing en beperkt is tot een bepaalde termijn (verlenging is mogelijk).
- De toegang beperkt is tot de doeleinden waarvoor het bevel is uitgevaardigd.

De algemene en ongedifferentieerde real-time- verwerking van verkeers- en locatiegegevens via geautomatiseerde analyse is mogelijk, indien:

- Geautomatiseerde analyse is beperkt tot situaties waarin een lidstaat wordt geconfronteerd met een "ernstige bedreiging van de nationale veiligheid die aantoonbaar reëel en actueel of voorzienbaar is"
- Een dergelijke analyse het voorwerp kan uitmaken van een "effectieve toetsing, hetzij door een rechter, hetzij door een onafhankelijke administratieve instantie waarvan de beslissing bindend is, met als doel na te gaan of er sprake is van een situatie die deze maatregel rechtvaardigt en of de voorwaarden en waarborgen die in acht moeten worden genomen".
- De vooraf vastgestelde modellen en criteria ten behoeve van een geautomatiseerde analyse "specifiek en betrouwbaar" zijn (waardoor resultaten kunnen worden verkregen waarmee personen kunnen worden geïdentificeerd die redelijkerwijs verdacht kunnen worden van deelname aan terroristische misdrijven), "niet-discriminerend", en "niet geïsoleerd op die gevoelige gegevens kunnen worden gebaseerd".
- Elk positief resultaat van geautomatiseerde verwerking "aan een individueel heronderzoek met niet-geautomatiseerde middelen wordt onderworpen voordat een voor de betrokkenen nadelige individuele maatregel wordt genomen, zoals het achteraf in real time verzamelen van verkeers- en locatiegegevens, aangezien een dergelijke maatregel niet uitsluitend en beslissend op het resultaat van geautomatiseerde verwerking kan worden gebaseerd".
- Regelmatig opnieuw wordt onderzocht of deze vooraf vastgestelde modellen en criteria en de gebruikte databanken betrouwbaar en actueel zijn.
- De bevoegde nationale instantie "verplicht is algemene informatie over deze analyse bekend te maken zonder de betrokkenen daarvan individueel in kennis te stellen". Indien echter "de gegevens overeenstemmen met de parameters die zijn gespecificeerd in de maatregel die toestemming geeft voor geautomatiseerde analyse en deze autoriteit de betrokkene identificeert om de hem of haar betreffende gegevens grondiger te analyseren, moet deze persoon wel individueel in kennis worden gesteld. Deze kennisgeving mag echter slechts plaatsvinden in de mate waarin en zodra zij de taken waarvoor deze autoriteiten verantwoordelijk zijn, niet meer in gevaar kan brengen".

Ten slotte wat betreft het gericht real-time verzamelen van verkeers- en locatiegegevens die uitsluitend betrekking hebben op een of meerdere personen, is dit mogelijk indien:

- Het gebruik van het realtime verzamelen van verkeers- en locatiegegevens is beperkt tot personen ten aanzien van wie een gegrond vermoeden bestaat dat zij op enigerlei wijze betrokken zijn bij terroristische activiteiten.
- Een "voorafgaande toetsing door een rechter of een onafhankelijk administratief orgaan" mogelijk is, waarvan de beslissing bindend is, teneinde te waarborgen dat deze realtime inzameling alleen wordt toegestaan binnen de grenzen van het strikt noodzakelijke. In naar behoren gemotiveerde dringende gevallen moet de toetsing op korte termijn plaatsvinden.

- Het besluit waarbij het real-time verzamelen van verkeers- en locatiegegevens wordt toegestaan "is gebaseerd op objectieve criteria die in de nationale wetgeving zijn vastgesteld". Die wetgeving moet met name bepalen "in welke omstandigheden en onder welke voorwaarden een dergelijke verzameling kan worden toegestaan en dat, zoals in het vorige punt is opgemerkt, alleen personen die verband houden met de doelstelling van preventie van terrorisme aan een dergelijke verzameling kunnen worden onderworpen" en "gebaseerd zijn op objectieve en niet-discriminerende criteria".
- De bevoegde nationale autoriteiten die realtime verkeers- en locatiegegevens verzamelen, moeten de betrokken personen daarvan overeenkomstig de toepasselijke nationale procedures in kennis stellen "voor zover en zodra die kennisgeving de taken waarvoor die autoriteiten verantwoordelijk zijn, niet langer in gevaar kan brengen".

3.3.4. C-764/18 – Prokuratuur

55. **FEITEN –** De betrokkene in de zaak Prokuratuur was veroordeeld tot een vrijheidsstraf van twee jaar. De vermeende strafbare feiten waren diefstallen met de bankkaart van een andere persoon en gewelddaden tegen een bij de procedure betrokken persoon.[215] De processen-verbaal waarop de vaststelling van die strafbare feiten was gebaseerd, waren opgesteld op basis van persoonsgegevens die in de loop van de onderzoeksprocedure verzameld werden door de opsporingsdienst bij een aanbieder van elektronische-communicatiediensten.[216] Het Estse openbaar ministerie had hiertoe steeds toestemming gegeven. De Estse wet verplicht de aanbieders om verkeers- en locatiegegevens algemeen en zonder onderscheid gedurende een jaar op te slaan. Deze verplichting betreft de volgende gegevens: naam en adres van beide partijen van het gesprek, datum en tijd van het begin en einde van het gesprek, het gebruikte toestel, de cel-ID bij het begin van het gesprek en de geografische locatie. Volgens het nationale recht kan toegang tot de gegevens worden verleend als dat essentieel is voor gebruik in een strafprocedure.[217] Vervolgens werd het vonnis aangevochten wegens niet rechtmatig verkregen bewijs. Het hof van beroep wees de vordering af. Het Estse Hooggerechtshof (Riigikohus) verwees de zaak naar het Hof van Justitie met het verzoek om uitlegging van art. 15, lid 1, van de e-Privacy Richtlijn.[218] Er zijn twee belangrijke vragen die het Estse Hooggerechtshof voor het Hof van Justitie heeft opgeworpen. Het Hooggerechtshof vroeg in hoeverre de duur van het verlenen van toegang tot bewaarde persoonsgegevens (communicatiemetadata) aan overheidsinstanties met het oog op onderzoek naar vermeende criminele gedragingen een rol speelt bij het bepalen of een dergelijke verlening van toegang een ernstige inbreuk vormt op het recht op privacy en gegevensbescherming, zoals verankerd in de artikelen 7 en 8 van het EU-Handvest. De tweede vraag had betrekking op de criteria die bepalen welke autoriteit onafhankelijk is, zodat zij toezicht kan houden op het verlenen van toegang tot bewaarde

[215] Prokuratuur, overw. 1.
[216] Prokuratuur, overw. 2.; I. REVOLIDIS, "H.K. v Prokuratuur: On Balancing Crime INvestigation and Data Protection", *EDPL* 2020, (319) 319-320.
[217] Prokuratuur, overw. 3.
[218] Prokuratuur, overw. 4.

persoonsgegevens aan andere autoriteiten ten behoeve van de opsporing, het onderzoek en de vervolging van strafbare feiten.

56. **ANALYSE VAN HET HOF –** De rechter verwijst naar zijn eerdere rechtspraak en stelt dat het bewaren van verkeers- en locatiegegevens een ernstige inbreuk op de grondrechten van het Handvest vormt. Ernstige inmenging doet zich voor ongeacht of de opslag een algemeen, willekeurig of doelgericht karakter heeft. De in casu op te slaan verkeers- en locatiegegevens maken precieze conclusies mogelijk over het privéleven van personen. Er kunnen conclusies worden getrokken over dagelijkse gewoonten, vaste of tijdelijke verblijfplaatsen, dagelijkse of andere regelmatige verplaatsingen, verrichte activiteiten en informatie over sociale betrekkingen en de sociale omgeving.[219] In het arrest beoordeelt het Hof van Justitie ook de vereisten van een onafhankelijke autoriteit volgens het Unierecht[220], namelijk of een openbaar ministerie dat het onderzoek uitvoert en eventueel de vervolging instelt, aan deze vereisten zou voldoen. Zoals in eerdere beslissingen van het Hof van Justitie is opgemerkt, moeten de voorwaarden betreffende de omstandigheden waarin toegang tot de gegevens wordt verleend, worden geregeld in het nationale recht.[221] Het evenredigheidsvereiste vereist echter dat de verordening duidelijk en nauwkeurig het toepassingsgebied en de toepassing van de maatregel vaststelt en de minimumvereisten beschrijft. Alleen op die manier krijgen de betrokkenen voldoende garanties voor een adequate bescherming tegen misbruik. De nationale regeling moet bindend zijn.[222] Niet alleen moet het doel voldoen aan art. 15, lid 1, maar ook moeten de materiële en procedurele voorwaarden voor het gebruik van de gegevens worden vastgesteld.[223] De algemene toegang tot alle opgeslagen gegevens is niet beperkt tot het strikt noodzakelijke. Daarom moet de nationale regelgeving ervoor zorgen dat de vaststelling van de omstandigheden en voorwaarden voor toegang tot gegevens gebaseerd is op objectieve criteria. Toegang tot verkeers- en locatiegegevens mag alleen worden verleend met het oog op de vervolging van ernstige strafbare feiten, nationale veiligheidsbelangen, nationale defensie of de openbare veiligheid.[224]

Om aan deze voorwaarden te voldoen, moet de toegang tot gegevens worden onderworpen aan een voorafgaande controle door een rechter of een bevoegde administratieve instantie. Deze voorafgaande controle vereist dat de bevoegde instantie over alle bevoegdheden en waarborgen beschikt die nodig zijn om ervoor te zorgen dat met tegenstrijdige belangen rekening kan worden gehouden. Dit betekent dat de rechter of het orgaan in het geval van een strafrechtelijk onderzoek een billijk evenwicht moet kunnen vinden tussen het belang van het onderzoek naar criminaliteit en de grondrechten van eerbiediging van het privéleven en bescherming van persoonsgegevens.[225] Het orgaan moet zijn taak dus objectief en onpartijdig uitvoeren, zonder

[219] Prokuratuur, overw. 44.; P. AERTGEERTS, "Bewaring van persoonsgegevens en de strijd tegen criminaliteit: een nieuw hoofdstuk" (noot onder HvJ 2 maart 2021, nr. C-764/18, ECLI:EU:C:2021:152, Prokuratuur), *TBP* 2022, (537) 538.
[220] Prokuratuur, overw. 46
[221] Prokuratuur, overw. 47.
[222] Prokuratuur, overw. 48.
[223] Prokuratuur, overw. 49.
[224] Prokuratuur, overw. 50.
[225] Prokuratuur, overw. 51.; P. AERTGEERTS, "Bewaring van persoonsgegevens en de strijd tegen criminaliteit: een nieuw hoofdstuk" (noot onder HvJ 2 maart 2021, nr. C-764/18, ECLI:EU:C:2021:152, Prokuratuur), *TBP* 2022, (537) 539.

invloed van andere partijen.[226] Dit betekent enerzijds dat het bevoegde orgaan niet betrokken mag zijn bij de onderzoeksprocedure en anderzijds dat het een neutrale houding aanneemt tegenover de partijen in het strafproces.[227] Het Estse openbaar ministerie, dat vooronderzoeken verricht en het publiek vertegenwoordigt bij vervolgingen, is niet onafhankelijk zoals het EU-recht vereist. Het kan geen onafhankelijke beslissingen nemen over bewijsmateriaal wanneer het een zaak voor de rechter moet brengen. Het OM is verplicht de belastende en ontlastende aspecten van het bewijsmateriaal te onderzoeken en is slechts gebonden aan de wet. Deze beperkingen zijn echter onvoldoende om de belangen adequaat af te wegen alsof zij door een derde worden gewogen.[228] Bovendien kan de latere rechterlijke toetsing dit gebrek aan onafhankelijke toetsing niet compenseren, aangezien de voorafgaande controle tot doel heeft ervoor te zorgen dat alleen de noodzakelijke gegevens openbaar worden gemaakt.[229] Het oordeel is dan ook dat een instantie als het Openbaar Ministerie, die het vooronderzoek verricht, de nodige onafhankelijkheid ontbeert om een onbevooroordeelde voorafgaande toetsing van de toegang tot gegevens te waarborgen.

57. **CONCLUSIE –** Het Hof bevestigt dat de mogelijkheid om toegang te krijgen afhankelijk is van het type van bewaarde gegevens. Toegang tot locatie– en verkeersgegevens vormt een ernstigere beperking van het recht op privacy en de bescherming van persoonsgegevens dan bijvoorbeeld toegang tot identificatiegegevens. Het openbaar ministerie kan daarom wel toegang krijgen tot identificatiegegevens, maar niet rechtstreeks tot locatie – en verkeersgegevens. Tot deze gegevens kan er enkel toegang worden genomen na een toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteiten, die hun beslissing over toegang tot locatie – en verkeersgegevens ook motiveren. Het Hof benadrukt dat wanneer deze toetsing niet door een rechterlijke instantie maar door een onafhankelijke bestuurlijke entiteit gebeurd, deze autoriteit onafhankelijk moet zijn, wat volgens het Hof betekent dat de autoriteit geen belang mag hebben ten aanzien van de andere partijen en niet betrokken is in het strafrechtelijk onderzoek. Daarom oordeelde het Hof van Justitie dat het openbaar ministerie onvoldoende afhankelijk is om deze gegevens op te vragen, omdat deze autoriteit in een later fase de verdachte zal vervolgen en dus belang heeft bij een brede dataretentie. Dit is ook het geval indien op het openbaar ministerie de verplichting rust om te bewijzen à charge en à décharge te verzamelen en functioneel onafhankelijk is ten aanzien van de minister van justitie. Enkel in het geval van urgentie kan het openbaar ministerie toegang nemen tot deze gegevens bij gemotiveerde beslissing waarbij de toetsing door de rechterlijke instantie zo snel mogelijk moet volgen.

[226] Prokuratuur, overw. 52.
[227] Prokuratuur, overw. 53.
[228] Prokuratuur, overw. 54.; .; P. AERTGEERTS, "Bewaring van persoonsgegevens en de strijd tegen criminaliteit: een nieuw hoofdstuk" (noot onder HvJ 2 maart 2021, nr. C-764/18, ECLI:EU:C:2021:152, Prokuratuur), *TBP* 2022, (537) 539.
[229] Prokuratuur, overw. 55.

3.3.5. C-140/20 – Commissioner de la Garde Síochána

58. **FEITEN –** In maart 2015 werd G.D. veroordeeld voor moord en kreeg hij een levenslange gevangenisstraf.[230] Hij heeft in beroep tegen zijn veroordeling bij het Court of Appeal in Ierland aangevoerd dat de rechter in eerste aanleg verkeers- en locatiegegevens van telefoongesprekken onterecht als bewijs heeft gebruikt. G.D. heeft bij de High Court (rechter in eerste aanleg, Ierland) een civiele procedure ingesteld waarin hij is opgekomen tegen enkele bepalingen van "the 2001 Act".[231] Bij beslissing van 6 december 2018 heeft de High Court het verzoek van G.D. toegewezen en geoordeeld dat section 6, lid 1, onder a), van deze wet in strijd was met artikel 15, lid 1, van de e-Privacy Richtlijn gelezen in het licht van de artikelen 7 en 8 en artikel 52, lid 1, van het EU-Handvest.[232] Ierland heeft tegen die beslissing beroep ingesteld bij de Supreme Court (hoogste rechterlijke instantie, Ierland), de verwijzende rechter.[233] Ierland heeft tegen dit besluit beroep ingesteld bij de Supreme Court, die de behandeling van de zaak heeft opgeschort en zes vragen heeft voorgelegd aan het Hof van Justitie.[234] Met zijn eerste, tweede en vierde vraag wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van e-Privacy Richtlijn, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid l, van het EU-Handvest, zich verzet tegen een nationale regeling die voor de bestrijding van zware criminaliteit, zoals doodslag, voorziet in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens.[235] Met zijn derde vraag wenst de verwijzende rechter te vernemen of diezelfde bepalingen zich verzetten tegen nationale wetgeving op grond waarvan de gecentraliseerde behandeling van verzoeken om toegang tot bewaarde gegevens die de politie doet tijdens het onderzoek naar en de vervolging van ernstige strafbare feiten, is opgedragen aan een politiefunctionaris, bijgestaan door een binnen de politie opgerichte eenheid die een zekere mate van autonomie heeft bij de uitvoering van haar taak en waarvan de beslissingen later door een rechter kunnen worden getoetst.[236] Ten slotte wat betreft de vijfde en zesde vraag, wenst de verwijzende rechter te vernemen of een nationale rechter in het licht van het Unierecht de werking in de tijd mag beperken van de ongeldigverklaring van nationale wetgeving die aanbieders van elektronische-communicatiediensten een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens oplegt, die hij op grond van het nationale recht dient uit te spreken wegens de onverenigbaarheid van die wetgeving met artikel 15, lid 1, van de e-Privacy Richtlijn, gelezen in het licht van het EU-Handvest.[237]

59. **ANALYSE VAN HET HOF –** Met betrekking tot de vragen 1,2 en 4 herhaalt het Hof van Justitie zijn vaste rechtspraak dat verkeers- en locatiegegevens betreffende elektronische communicatie niet algemeen en zonder onderscheid mogen worden bewaard met het oog op de bestrijding van zware criminaliteit. Het Hof van Justitie haalt drie onderliggende redenen aan waarom de strijd

[230] Commissioner of An Garda Síochána, overw. 20.
[231] Commissioner of An Garda Síochána, overw. 21.
[232] *Ibid.*
[233] Commissioner of An Garda Síochána, overw. 23.
[234] Commissioner of An Garda Síochána, overw. 30.
[235] Commissioner of An Garda Síochána, overw. 31.
[236] Commissioner of An Garda Síochána, overw. 102.
[237] Commissioner of An Garda Síochána, overw. 105.

tegen ernstige criminaliteit niet hetzelfde is als de bescherming van de nationale veiligheid.[238] Ten eerste heeft het Hof in dit verband geoordeeld dat het belang van de doelstelling van bescherming van de nationale veiligheid tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd.[239] Ten tweede heeft het Hof ook reeds geoordeeld dat de doelstelling de nationale veiligheid te beschermen, strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en het voorkomen en bestrijden van activiteiten omvat 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. Ten derde wijst het Hof erop dat een bedreiging voor de nationale veiligheid reëel en actueel of op zijn minst voorzienbaar moet zijn, wat veronderstelt dat er voldoende concrete aanwijzingen zijn om te kunnen rechtvaardigen dat een maatregel wordt genomen om verkeers- en locatiegegevens gedurende een beperkte periode algemeen en ongedifferentieerd te bewaren. Een dergelijke bedreiging verschilt dus door haar aard, haar ernst en het bijzondere karakter van de omstandigheden waarin zij zich voordoet, van het algemene, permanente risico op – zelfs ernstige – spanningen of wanordelijkheden die de openbare veiligheid ondermijnen of ernstige strafbare feiten.[240] Daardoor, besluit het Hof dat de strijd tegen criminaliteit, ook ernstige criminaliteit, onvoldoende uitzonderlijk en periodiek is om een dergelijke algemene beperking voor de hele bevolking op het recht op privacy en de bescherming van persoonsgegevens te verantwoorden.[241] In dit verband herhaalt het Hof van Justitie uitvoerig zijn vorige rechtspraak en verduidelijkt het nogmaals welke wettelijke maatregelen ten behoeve van de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid zijn toegelaten.

Met betrekking tot de derde vraag stelt het Hof dat een nationale regeling, om te voldoen aan de proportionaliteitsvereisten, duidelijk en nauwkeurig het toepassingsgebied en de toepassing van de betrokken maatregel moet regelen en minimumwaarborgen moet bieden die de bescherming van deze gegevens voldoende waarborgen.[242] Om de naleving van de strikte voorwaarden te waarborgen, moeten nationale autoriteiten die toegang tot dergelijke gegevens wensen, onderworpen worden aan een voorafgaande toetsing door een rechtbank of een onafhankelijk administratief orgaan.[243] Een politiefunctionaris vormt niet zo'n administratief orgaan, aangezien voor hem niet dezelfde waarborgen van onafhankelijkheid en onpartijdigheid gelden.[244] Bijgevolg dient op de derde vraag te worden geantwoord dat artikel 15, lid 1 van de e-Privacy Richtlijn gelezen in het licht van het EU-Handvest, aldus moet worden uitgelegd dat

[238] C. VAN DE HEYNING, "Het moeilijke evenwicht tussen privacy & veiligheid: De impact van het debat over bewaren van communicatiegegevens", *Radices* 2022, (132) 143.
[239] Commissioner of An Garda Síochána, overw. 57.
[240] Commissioner of An Garda Síochána, overw. 62.
[241] Commissioner of An Garda Síochána, overw. 63-64.
[242] Commissioner of An Garda Síochána, overw. 104-108.
[243] *Ibid.*
[244] Commissioner of An Garda Síochána, overw. 111.

het zich verzet tegen nationale wetgeving op grond waarvan de gecentraliseerde behandeling van verzoeken om toegang tot door aanbieders van elektronische-communicatiediensten bewaarde gegevens die de politie doet tijdens het onderzoek naar en de vervolging van ernstige strafbare feiten, is opgedragen aan een politiefunctionaris, bijgestaan door een binnen de politie opgerichte eenheid die een zekere mate van autonomie heeft bij de uitvoering van haar taak en waarvan de beslissingen later door een rechter kunnen worden getoetst.[245]

Ten slotte heeft het Hof geoordeeld dat het Unierecht zich ertegen verzet dat een nationale rechter de werking in de tijd beperkt van een ongeldigverklaring die hij krachtens het nationale recht dient af te geven "met betrekking tot een nationale regeling die aanbieders van elektronische-communicatiediensten een algemene en willekeurige bewaring van verkeers- en locatiegegevens oplegt".[246] In dit verband verduidelijkt het Hof ook dat, gelet op het beginsel van procedurele autonomie van de lidstaten, de toelaatbaarheid van door middel van een dergelijke bewaring verkregen bewijs een zaak van nationaal recht is.[247]

60. **CONCLUSIE –** Het Hof van Justitie voegt een nieuw hoofdstuk toe aan het lange verhaal over dataretentie in de Europese Unie en bevestigt bij dit arrest zijn vaste rechtspraak dat de strijd tegen (ernstige) criminaliteit onvoldoende is om een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens te rechtvaardigen.

3.3.6. C-793/19 en C-794/19 – SpaceNet en Telekom Deutschland en C-339/20 en C-397/20 VD en SR

61. **FEITEN –** In Duitsland bieden SpaceNet en Telekom Deutschland openbare internettoegangsdiensten aan, terwijl Telekom Deutschland ook telefoondiensten aanbiedt.[248] Zij hebben bij de Duitse rechter beroep ingesteld tegen de verplichting die de Duitse telecommunicatiewet hen oplegt om vanaf 1 juli 2017 verkeers- en locatiegegevens met betrekking tot de telecommunicatie van hun klanten te bewaren, behalve in enkele uitzonderlijke gevallen.[249] Volgens de wet moeten aanbieders van openbare elektronische communicatiediensten in het algemeen de meeste verkeers- en locatiegegevens van hun eindgebruikers gedurende enkele weken bewaren, zonder onderscheid te maken, om ernstige strafbare feiten te onderzoeken of om de nationale veiligheid te beschermen. Het Duitse Bundesverwaltungsgericht wil nagaan of deze nationale regeling in strijd is met het Unierecht, zoals geïnterpreteerd door het Hof van Justitie.[250] Het Bundesverwaltungsgericht twijfelt met name vanwege het feit dat de bewaarplicht van het TKG minder gegevens omvat en korter duurt

[245] Commissioner of An Garda Síochána, overw. 114.
[246] Commissioner of An Garda Síochána, overw. 129.
[247] Commissioner of An Garda Síochána, overw. 127.
[248] Spacenet, overw. 22.
[249] SpaceNet, overw. 23-24.
[250] SpaceNet, overw. 39.

(4 of 10 weken) dan de nationale regeling in eerdere zaken die tot de eerdere arresten van het Hof van Justitie hebben geleid.[251]

De zaken VD en SR betreffen onderzoeken tegen twee verdachten in Frankrijk omdat ze zouden gehandeld hebben met voorkennis, heling van handel met voorkennis, medeplichtigheid, omkoping en witwassen.[252] De AMF heeft in het kader van dat onderzoek persoonsgegevens uit telefoongesprekken van VD en SR gebruikt die op grond van de code des postes et des communications électroniques (wetboek posterijen en elektronische communicatie) waren verkregen in het kader van de levering van elektronischecommunicatiediensten.[253] De verwijzende Cour de Cassation vroeg zich af of er een onafhankelijke verplichting bestaat voor de nationale wetgever om van de aanbieders van elektronische communicatiediensten te vereisen om tijdelijk maar op algemene basis deze gegevens te bewaren, om de administratieve autoriteit in staat te stellen te voldoen aan secundaire EU-wetgeving over marktmisbruik.[254] Met haar verzoek om een prejudiciële beslissing vraagt de Cour de Cassation het Hof van Justitie in wezen hoe de relevante bepalingen van de "richtlijn betreffende privacy en elektronische communicatie", gelezen in het licht van het EU-Handvest in overeenstemming kunnen worden gebracht met de relevante bepalingen van de "richtlijn marktmisbruik" en de "verordening marktmisbruik" in de context van bepalingen van nationaal recht die, bij wijze van preventieve maatregel ter bestrijding van marktmisbruik, waaronder handel met voorkennis, voorzien in de algemene en ongedifferentieerde bewaring van verkeersgegevens door exploitanten die elektronische-communicatiediensten aanbieden, gedurende een jaar vanaf de datum waarop zij zijn geregistreerd.[255]

62. **ANALYSE VAN HET HOF** – Met betrekking tot het arrest SpaceNet, is het aan het Hof om te bepalen of de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens met het oog op de bestrijding van ernstige criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid gerechtvaardigd is voor een korte periode van opslag.[256] Het Hof van Justitie beoordeelt dit in het licht van de ernst van de inmenging, die nader wordt geoperationaliseerd door in hoeverre door de opgeslagen gegevens een zeer precies beeld over het privéleven van een gebruiker van een elektronisch communicatiemiddel wordt verschaft.[257] Het is, volgens het Hof van Justitie EU, namelijk de bewaring die al een ernstige inmenging in het te beschermen privéleven veroorzaakt, doordat die bewaring de noodzakelijke voorwaarde is voor toegang tot de gegevens en door de opslag het risico ontstaat dat zeer precieze conclusies over eindgebruikers privéleven kunnen worden getrokken. Het antwoord dus op de gestelde vraag duidelijk negatief. Ten behoeve van de bestrijding van zware criminaliteit is alleen *gerichte*

[251] D. VAN TOOR, "SpaceNet en VD (HvJ EU, C-793/19 en C-339/20) – Here we go again: Duitse en Franse dataretentieregeling(en) in strijd met Unierecht", *European Human Rights Cases Updates* 2023, www.ehrc-updates.nl/commentaar/212435?skip_boomportal_auth=1.
[252] VD, overw. 2.
[253] X. TRACOL, "The Joined cases of Dwyer, SpaceNet and VD and SR before the European Court of Justice: The Judgements of the Grand Chamber about data retention continue falling on deaf ears in Member States", *COMPUTER LAW&SECURITY REVIEW* 2023, (1) 2.
[254] *Ibid,* 3.
[255] VD, overw. 46.
[256] SpaceNet, overw. 85.
[257] Spacenet, overw. 89.

bewaring mogelijk, op basis van objectieve en niet-discriminatoire gronden, voor een periode niet langer dan strikt noodzakelijk.[258] Daarentegen verzet het Unierecht zich niet tegen een nationale wettelijke regeling:

- 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. Dat bevel kan worden getoetst door een rechter of een onafhankelijke bestuurlijke entiteit en kan slechts worden uitgevaardigd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd als die bedreiging blijft bestaan;

- Die met het oog op de bescherming van de nationale veiligheid, de bestrijding van *zware* criminaliteit en de voorkoming van *ernstige* bedreigingen voor de openbare veiligheid voorziet 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;

- Die voor dezelfde doeleinden voorziet 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 met het oog op de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorziet in een algemene en ongedifferentieerde bewaring van de gegevens die betrekking hebben op de burgerlijke identiteit van de gebruikers van elektronische- communicatiemiddelen, en

- Die met het oog op de bestrijding van *zware* criminaliteit en, a fortiori, de bescherming van de nationale veiligheid voorziet in de mogelijkheid om aan aanbieders van elektronische-communicatiediensten een bevel te geven tot spoedbewaring, gedurende een bepaalde periode, van de verkeers- en locatiegegevens waarover zij beschikken.

Een dergelijke nationale wettelijke regeling moet bovendien, 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 dat de betrokken personen beschikken over effectieve waarborgen tegen de risico's op misbruik.

[258] Spacenet, overw. 131.; X. TRACOL, "The Joined cases of Dwyer, SpaceNet and VD and SR before the European Court of Justice: The Judgements of the Grand Chamber about data retention continue falling on deaf ears in Member States", *COMPUTER LAW&SECURITY REVIEW* 2023, (1) 7.

63. Met betrekking tot het arrest VD en SR, stelt het Hof van Justitie ten eerste vast dat noch de richtlijn marktmisbruik, noch de verordening marktmisbruik de rechtsgrondslag kan vormen voor een algemene verplichting om de gegevens over het verkeer die in het bezit zijn van operatoren die elektronische-communicatiediensten aanbieden, te bewaren met het oog op de uitoefening van de bevoegdheden die krachtens deze maatregelen aan de bevoegde financiële autoriteiten zijn toegekend.[259] In de tweede plaats herinnert het Hof eraan dat de e-Privacy Richtlijn de referentiemaatstaf is voor de bewaring en, meer in het algemeen, de verwerking van persoonsgegevens in de sector elektronische communicatie.[260] Deze richtlijn regelt dus ook de verkeersgegevens die worden bijgehouden door exploitanten van elektronische-communicatiediensten, en die de bevoegde financiële autoriteiten in de zin van de richtlijn inzake marktmisbruik en de verordening inzake marktmisbruik van deze exploitanten kunnen verlangen.[261] Bijgevolg moet de rechtmatigheid van de verwerking van de gegevens worden getoetst aan de voorwaarden van de e-Privacy Richtlijn. Het Hof stelt vervolgens vast dat de richtlijn marktmisbruik en de verordening marktmisbruik, gelezen in samenhang met de e-Privacy Richtlijn en in het licht van het EU-Handvest, niet toestaan dat exploitanten die elektronische-communicatiediensten aanbieden verkeersgegevens algemeen en zonder onderscheid bewaren gedurende een jaar vanaf de datum waarop zij zijn geregistreerd met het oog op de bestrijding van marktmisbruik, waaronder handel met voorkennis.[262] Ten slotte bevestigt het Hof zijn rechtspraak volgens welke het Unierecht zich ertegen verzet dat een nationale rechter de werking in de tijd beperkt van een nietigverklaring die hij krachtens het nationale recht moet uitspreken over een nationale regeling die de exploitanten van elektronische-communicatiediensten verplicht tot het algemeen en zonder onderscheid bewaren van verkeers- en locatiegegevens, omdat deze regeling onverenigbaar is met de e-Privacy Richtlijn.[263]

64. **CONCLUSIE -** In de twee SpaceNet en VD en SR heeft de Grote kamer hoofdzakelijk haar eigen toepasselijke rechtspraak over het bewaren van en de toegang tot verkeers- en locatiegegevens herhaald. In het arrest VD en SR heeft de Grote kamer echter haar werkingssfeer uitgebreid tot het gebied van marktmisbruik door vast te stellen dat de e-privacyrichtlijn van toepassing is op de verkeersgegevens die worden bijgehouden door exploitanten die elektronische-communicatiediensten aanbieden en die de bevoegde financiële autoriteiten in de zin van zowel de richtlijn als de verordening inzake marktmisbruik van deze exploitanten kunnen verlangen.

[259] VD, overw. 78.; D. VAN TOOR, "SpaceNet en VD (HvJ EU, C-793/19 en C-339/20) – Here we go again: Duitse en Franse dataretentieregeling(en) in strijd met Unierecht", *European Human Rights Cases Updates* 2023, www.ehrc-updates.nl/commentaar/212435?skip_boomportal_auth=1.
[260] *Ibid.*
[261] VD, overw. 73.
[262] VD, overw. 89.
[263] VD, overw. 108.

3.4. Synthese

Tabel 1 – Overzicht op basis van de soorten gegevens

Bewaring	**Doelstelling (art. 15, lid 1 e-Privacy Richtlijn en arresten)**
Algemene en ongedifferentieerde bewaring van identificatiegegevens (niet-ernstige inmenging)	Waarborging van de nationale veiligheid Waarborging van de openbare veiligheid en de bestrijding van ernstige criminaliteit Bestrijding van criminaliteit in het algemeen
Algemene en ongedifferentieerde bewaring van IP-adressen ter identificatie van de gebruiker (ernstige inmenging)	Waarborging van de nationale veiligheid Waarborging van de openbare veiligheid en de bestrijding van ernstige criminaliteit
Algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens (bijzonder ernstige inmenging)	Waarborging van de nationale veiligheid

65. **TOELICHTING –** Deze tabel geeft onder "bewaring" de soort bewaring aan per communicatiegegeven. Het gaat met name over identificatiegegevens, IP-adressen en verkeers- en locatiegegevens. Deze bewaringsplichten kunnen enkel worden ingevoerd overeenkomstig de doelstellingen uitgeschreven in het corresponderend kader onder "doelstelling". Ze zijn gerangschikt van niet-ernstige inmenging naar bijzonder ernstige inmenging. Deze tabel vindt ook steun in de rechtsleer. Zo hanteren VAN ROY[264], ROYER[265] en KEUNEN[266] een gelijkaardig schematisch overzicht. Wat betreft de koppeling van de soort bewaring aan de doelstelling, is deze gestoeld op een algemene consensus in de rechtsleer. Hier kan er verwezen worden naar verschillende bijdragen van onder andere VAN DE HEYNING, PANZAVOLTA, VAN ROY en ROYER. Wanneer er verder wordt gekeken dan bijdragen verschenen in Belgische literatuur, leert een blik over de landsgrens dat deze consensus ook op Europees niveau gedragen wordt. Hierbij kan er verwezen worden naar onder andere verschillende bijdragen van CAMERON, TRACOL en ESKENS.

[264] L. VAN ROY en S. ROYER, "De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep", *NC* 2023, (1) 22.
[265] *Ibid.*
[266] L. KEUNEN, "De vernietiging van de Dataretentiewet 2.0: naar een gerichte bewaring met ruimere toegang?" (noot onder GwH 22 april 2021, nr. 57/2021), *RWE* 2021-22, (1464) 1470.

Tabel 2 – Overzicht van de bewaarplichten, de doelstellingen die ze nastreven en de voorwaarden die moeten voldaan zijn.

Doelstelling	**Bewaarplicht**	**Voorwaarden**
Concrete aanwijzingen van een reële en actuele of voorzienbare ernstige dreiging van de nationale veiligheid	Preventieve algemene bewaring van verkeers- en locatiegegevens	- Beperkt in de tijd (verlenging mogelijk) - Onderworpen aan een effectieve toetsing, hetzij door een rechtbank, hetzij door een onafhankelijke administratieve instantie waarvan de beslissing bindend is - Toetsing heeft tot doel na te gaan of een van deze situaties zich voordoet en of de voorwaarden en waarborgen die moeten worden gesteld, in acht worden genomen.
	Preventieve gerichte bewaring van verkeers- en locatiegegevens	- Op basis van objectieve en niet-discriminerende factoren - De duur is niet langer dan strikt noodzakelijk in het licht van het nagestreefde doel en de omstandigheden (verlenging is mogelijk)
	Preventieve algemene bewaring van burgerlijke identiteitsgegevens	- Uitsluitend gericht op de identificatie van de betrokken gebruiker - Gegevens mogen niet in verband kunnen worden gebracht met informatie over de gedane mededelingen - Zelfs wanneer de wetgeving geen specifieke termijn oplegt
	Real-time bewaring van verkeers- en locatiegegevens	- Beperkt tot personen ten aanzien van wie een gegrond vermoeden bestaat dat zij op enigerlei wijze betrokken zijn bij terroristische activiteiten. - Een voorafgaande toetsing door een rechter of een onafhankelijk administratief orgaan, waarvan de beslissing bindend is, teneinde te waarborgen dat deze realtime inzameling alleen wordt toegestaan binnen de grenzen

		van het strikt noodzakelijke. In naar behoren gemotiveerde dringende gevallen moet de toetsing op korte termijn plaatsvinden. - Het besluit waarbij het real-time verzamelen van verkeers- en locatiegegevens wordt toegestaan is gebaseerd op objectieve criteria die in de nationale wetgeving zijn vastgesteld. Die wetgeving moet met name bepalen in welke omstandigheden en onder welke voorwaarden een dergelijke verzameling kan worden toegestaan en dat, zoals in het vorige punt is opgemerkt, alleen personen die verband houden met de doelstelling van preventie van terrorisme aan een dergelijke verzameling kunnen worden onderworpen en gebaseerd zijn op objectieve en niet-discriminerende criteria. - De bevoegde nationale autoriteiten die realtime verkeers- en locatiegegevens verzamelen, moeten de betrokken personen daarvan overeenkomstig de toepasselijke nationale procedures in kennis stellen "voor zover en zodra die kennisgeving de taken waarvoor die autoriteiten verantwoordelijk zijn, niet langer in gevaar kan brengen.
	Versnelde bewaring van verkeers- en locatiegegevens	- Het bevel tot versnelde bewaring moet worden uitgevaardigd door de bevoegde autoriteit zoals bepaald in het recht van de lidstaat. - Het bevel is onderworpen aan effectieve rechterlijke toetsing en is beperkt tot een bepaalde termijn (verlenging is mogelijk).

		- De toegang is beperkt tot de doeleinden waarvoor het bevel is uitgevaardigd.
Bestrijding van ernstige criminaliteit, voorkoming van "ernstige bedreigingen" of "ernstige aanslagen" op de openbare veiligheid (en *a fortiori* de nationale veiligheid)	Preventieve gerichte bewaring van verkeers- en locatiegegevens	- De gerichte bewaring wordt beperkt op basis van objectieve en niet-discriminerende factoren. De beperkingen kunnen: Worden vastgesteld volgens de categorieën van betrokken personen op basis van objectief bewijsmateriaal dat het mogelijk maakt zich te richten op personen wier verkeers- en locatiegegevens waarschijnlijk een verband, althans een indirect verband, met ernstige strafbare feiten aan het licht zullen brengen; of - Aan de hand van een geografisch criterium dat is vastgesteld op basis van objectieve en niet-discriminerende factoren - De duur is niet langer dan strikt noodzakelijk in het licht van het nagestreefde doel en de omstandigheden die deze rechtvaardigen (verlenging is mogelijk)
	Preventieve algemene bewaring van IP-adressen	- De bewaartermijn is niet langer dan strikt noodzakelijk is in het licht van het nagestreefde doel". - De maatregel stelt strikte voorwaarden en waarborgen vast voor het gebruik van deze gegevens, met name via tracking, met betrekking tot de door de betrokken personen gedane handelingen en onlineactiviteiten.
	Preventieve algemene en ongedifferentieerde bewaring van burgerlijke identiteitsgegevens	- Uitsluitend gericht op de identificatie van de betrokken gebruiker - De gegevens mogen niet in verband kunnen worden

		gebracht met informatie over de gedane mededelingen
	Versnelde bewaring van verkeers- en locatiegegevens	- Het bevel tot versnelde bewaring moet worden uitgevaardigd door de bevoegde autoriteit zoals bepaald in het recht van de lidstaat. - Het bevel is onderworpen aan effectieve rechterlijke toetsing en beperkt is tot een bepaalde termijn (verlenging is mogelijk). - De toegang is beperkt tot de doeleinden waarvoor het bevel is uitgevaardigd.
Bestrijding van criminaliteit in het algemeen en beschermen van de openbare orde	Preventieve algemene en ongedifferentieerde bewaring van burgerlijke identiteitsgegevens	- Uitsluitend gericht op de identificatie van de betrokken gebruiker - De gegevens mogen niet in verband kunnen worden gebracht met informatie over de gedane mededelingen

66. **TOELICHTING –** Deze tabel is een weergave van de verschillende bewaarplichten, de doelstellingen die ze moeten nastreven en de voorwaarden waaraan moet worden voldaan. De eerste kolom komt overeen met de doelstellingen opgesomd in artikel 15, lid 1 van de e-Privacy Richtlijn. De doelstellingen zijn gerangschikt van meest ernstige afwijking naar minst ernstige afwijking van het principe van vertrouwelijkheid. In de tweede kolom wordt een weergave gegeven per doelstelling van de bewaarplichten die kunnen ingevoerd worden op basis van de corresponderende doelstelling. In de laatste kolom wordt een schematisch overzicht gegeven van de voorwaarden waaraan de bewaarplicht moet voldoen om gerechtvaardigd te zijn in het licht van de na te streven doelstelling. Opnieuw vindt deze tabel steun in de rechtsleer. Zowel CAREEL en ROYER als KEUNEN komen namelijk tot een gelijkaardige synthese bij hun analyse van de arresten van het Hof van Justitie.

Tabel 3 – toegang tot gegevens

Communicatiegegevens	Toegang voor commerciële redenen	Toegang voor de bestrijding van ernstige criminaliteit en ter bescherming van de openbare veiligheid	Toegang voor bescherming nationale veiligheid
Bewaard voor commerciële reden	Ja	Ja	Ja
Bewaard voor de bestrijding van ernstige criminaliteit, voorkoming van "ernstige bedreigingen" of "ernstige aanslagen" op de openbare veiligheid	Nee	Ja	Ja
Bewaard voor bescherming nationale veiligheid	Nee	Nee	Ja

67. **TOELICHTING –** Het Hof van Justitie heeft een duidelijk onderscheid gemaakt tussen de bewaring van de gegevens en de toegang tot deze gegevens. Deze tabel focust op de toegang tot de communicatiegegevens. In de eerste kolom wordt een overzicht gemaakt van de doelstellingen op basis waarvan communicatiegegevens worden bewaard. In de eerste rij wordt daarentegen de verschillende soorten toegang voor die doelstellingen beschreven. De regel over de toegang tot gegevens door autoriteiten kan dan ook samengevat worden als 'qui peut le plus, peut le moins', zoals beschreven door VAN DEN HEYNING. Een autoriteit mag voor een bepaalde doelstelling wel toegang nemen tot gegevens bewaard voor een minder zwaarwichtige doelstellingen, maar niet tot gegevens be- waard voor een zwaarwichtigere doelstelling.

4. EVALUATIE VAN DE DATARETENTIEWET VAN 2022 IN HET LICHT VAN HET UNIERECHTELIJK KADER

4.1.Inleiding

68. **INLEIDING –** In dit hoofdstuk zal de nieuwe dataretentiewet van 2022 geëvalueerd worden in het licht van het Unierechtelijk kader, zoals uiteengezet in hoofdstuk 3. In bijlage 1 bij deze masterscriptie is een schematisch overzicht bijgevoegd van deze nieuwe dataretentiewet waarin snelle kruisverwijzingen worden aangeboden. Meer concreet zal dit hoofdstuk in de eerste plaats de voorgeschiedenis van de dataretentiewet van 2022 toelichten. Op deze manier is niet alleen het ruimer kader en de ontstaansgeschiedenis van de wet duidelijk, maar geeft het tegelijkertijd ook een beeld van de moeilijke intrede van dataretentie in België. Vervolgens zal de verenigbaarheid van vijf kernelementen van de Belgische dataretentiewet van 2022 met het Unierechtelijk kader besproken worden, namelijk: (i) het personeel toepassingsgebied, (ii) het materieel toepassingsgebied, (iii) de versleuteling, (iv) de bewaringsregimes en (vi) de toegang tot de bewaarde gegevens. Wat betreft het personeel toepassingsgebied zal er niet zozeer teruggekoppeld worden naar de arresten van het Hof van Justitie, maar een algemene analyse gemaakt worden aan de hand van recente wetgeving op EU-niveau en de memorie van toelichting. Dit is omdat de twistpunten in de mijlpaalarresten geen betrekking hadden op het personeel toepassingegebied. Bij de analyse van het materieel toepassingegebied wordt er gesteund op de arresten van het Hof van Justitie, op een vergelijking met het KB van 19 september 2013 en een recent arrest van het Grondwettelijk Hof in een gelijkaardige kwestie specifiek betrekking hebbende op het materieel toepassingegebied. Wat betreft de versleuteling, zal in beperkte mate het debat rond versleuteling op het niveau van de Europese Unie worden toegelicht. Vervolgens worden de bewaarregimes onderverdeeld in algemene bewaring en gerichte bewaring. Het uitgangspunt blijft de toetsing van de criteria uiteengezet in hoofdstuk 3. Deze toetsing wordt aangevuld door bijdragen in de rechtsleer, eigen inzichten en de verwerking van de gesprekken binnen het kader van *students@cuta.* Ten slotte wordt er voor de evaluatie van de toegang tot de bewaarde gegevens ook voortgebouwd op de criteria uiteengezet in hoofdstuk 3.

4.2. Voorgeschiedenis van de Belgische dataretentiewet van 2022

69. **WET VAN 28 NOVEMBER 2000 INZAKE INFORMATIECRIMINALITEIT –** Nog voordat de Europese Unie had opgetreden binnen het dataretentiegebied, bestond er in België reeds een gegevensbewaringsplicht. Deze bewaringsplicht was ingevoerd door de wet van 28 december 2000 inzake informatiecriminaliteit.[267] De wet in kwestie vulde zowel de regeling aan voor de interceptie van telecommunicatie die geregeld was bij de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie[268], als de artikelen 90*ter* tot en met 90*decies* van het Wetboek van Strafvordering[269] op hoofdzakelijk twee punten. Enerzijds werd de lijst van strafbare feiten die observatie en interceptie mogelijk maken uitgebreid met de in het Strafwetboek opgenomen strafbare feiten in verband met computers.[270] Anderzijds werd de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven[271] gewijzigd om de verplichting op te nemen om gespreksgegevens en identificatiegegevens van gebruikers van telecommunicatiemiddelen te registreren en op te slaan gedurende een termijn van 12 maanden.[272]

70. **WET BETREFFENDE DE ELEKTRONISCHE COMMUNICATIE (WEC) –** Eind jaren 90 werd de telecommunicatiesector onder Europese invloed geliberaliseerd. Dit leidde tot aanzienlijke wijzigingen binnen de betrokken sector.[273] Om deze redenen werd in 1999 op Europees vlak overgegaan tot een aanpassing van het regelgevende kader.[274] Dit resulteerde in de loop van het jaar 2002 in zes richtlijnen: vijf harmoniseringrichtlijnen en een specifieke richtlijn betreffende de mededinging op de markt- en voor elektronische communicatiediensten.[275] De telecommunicatieaspecten van deze zes richtlijnen worden door de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna: WEC of Telecomwet) in Belgisch recht omgezet.[276] Belangrijk hierbij is oorspronkelijk artikel 126 WEC. Dit artikel bepaalde dat verkeers- en identificatiegegevens gedurende 12 tot 36 maanden moesten worden bewaard met het oog op criminaliteitsbestrijding, de beteugeling van kwaadwillige oproepen naar de nooddiensten, het onderzoek naar personen die kwaadwillig gebruikmaken van elektronische communicatienetwerken of -diensten en de inlichtingenopdrachten.[277] Daarnaast bestond er reeds een Koninklijk Besluit dat uitvoering gaf aan bepaalde medewerkingsplichten. Het bepaalde

[267] Wet van 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001, 02.909.
[268] Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, *BS* 24 januari 1995, 1542.
[269] Wetboek van Strafvordering – Eerste boek van 17 november 1808, BS 27 november 1808, 0.
[270] F. DE VILLANFAGNE en S. DUSOLLIER, "La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique", *AM* 2001, (60) 78.
[271] Wet van 21 maart 1991 betreffende de hervorming van sommige overheidsbedrijven, *BS* 27 maart 1991, 6155.
[272] Art. 14 Wet 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001, 02.909.; In wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 2000-2001, nr. 50-0213/011, 18 werd reeds kritiek geuit op de afwezigheid van waarborgen tegen het risico op misbruik door de Europese Commissie.
[273] Wetsontwerp van 4 november 2004 betreffende de elektronische communicatie, *Parl.St.* Kamer 2004-2005, nr. 51-1425/001, 3.
[274] *Ibid.*
[275] *Ibid.*
[276] Wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 juni 2005, 28070.
[277] Wetsontwerp van 4 november 2004 betreffende de elektronische communicatie, *Parl.St.* Kamer 2004-05, nr. 51-1425/001 en 51-1426/001, 77-78.

onder meer dat elke dienstenaanbieder een coördinatiecel Justitie moest oprichten, die voor de aanvragen van gerechtelijke autoriteiten instond.[278]

71. **DATARETENTIEWET VAN 2013 –** De eerste Belgische dataretentiewet werd ingevoerd in 2013, als gevolg van de late implementatie van de Europese dataretentierichtlijn. Deze richtlijn bood een verbeterde bescherming aangezien deze strikter was dan de toen geldende wetgeving met betrekking tot het bewaren van telefoniegegevens en meer waarborgen bood voor de bescherming van deze gegevens. Concreet waren de nieuwe relevante bepalingen te vinden in zowel de Telecomwet als in het Wetboek van strafvordering, in het bijzonder de artikelen 46*bis* (opvragen van identificatiegegevens) en 88*bis* Sv. (opvragen van verkeers- en locatiegegevens). De wetgever heeft artikel 126 WEC aangepast om te voldoen aan de verplichtingen die de dateretentierichtlijn oplegde, waardoor er een duidelijke dataretentieplicht ontstond in de Belgische wetgeving.[279] De dataretentiewet van 2013 verklaarde de bepalingen van de Privacywet uitdrukkelijk van toepassing en beperkte het toepassingsgebied van de bewaarplicht tot aanbieders van vaste en mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie, en aanbieders van de onderliggende openbare elektronische communicatienetwerken.[280] De wet verduidelijkte verder dat de bewaarplicht enkel bestond voor zover de aanbieders de gegevens genereren of verwerken. Daarnaast werd het gebruik van dataretentie toegelaten voor vier verschillende doeleinden: de opsporing, het onderzoek en de vervolging van strafbare feiten; de bestraffing van kwaadwillige oproepen naar noodcentrales; het kwaadwillig gebruik van elektronische communicatiediensten of -netwerken en ten slotte opdrachten van veiligheids- en inlichtingendiensten.[281] De gegevens ter identificatie van de eindgebruikers, de gebruikte elektronische-communicatiedienst en de vermoedelijk gebruikte eindapparatuur worden bewaard vanaf de inschrijving op de dienst, zolang binnenkomende of uitgaande communicatie mogelijk is door middel van de dienst waarop werd ingetekend en gedurende 12 maanden vanaf de datum van de laatste geregistreerde binnenkomende of uitgaande communicatie.[282] De verkeers- en localisatiegegevens worden bewaard gedurende 12 maanden vanaf de datum van de communicatie.[283]

72. **GWH 11 JUNI 2015, NR. 84/2015 –** Het Grondwettelijk Hof vernietigde de eerste Belgische dataretentiewet amper twee jaar na de invoering ervan. Het Hof achtte deze wet strijdig met het gelijkheids- en non-discriminatiebeginsel gewaarborgd door artikel 10 en 11 van de Grondwet, in samenhang gelezen met artikel 7 en 8 van het EU-Handvest. Om tot deze conclusie te komen, baseerde het Hof zich op de overwegingen van het *Digital Rights Ireland*-arrest van het Hof van

[278] KB 9 januari 2003 tot uitvoering van de artikelen 46bis, § 2, eerste lid, 88*bis*, § 2, eerste en derde lid, en 90quater, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109*ter*, § 2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *BS* 10 februari 2003.
[279] M. PANZAVOLTA, S. ROYER en H. SEVERIJNS, "Algemene dataretentie: ten minste houdbaar tot…?", *T.Strafr.* 2018*,* (3) 6.
[280] *Ibid.*
[281] Wetsontwerp van 27 juni 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van Strafvordering, Parl.St. Kamer 2012-13, nr. 53-2921/001, 14.
[282] Oud art. 126 WEC.
[283] *Ibid.*

Justitie.[284] Ten eerste was volgens het Grondwettelijk Hof het ruime toepassingsgebied van de algemene bewaringsplicht problematisch. De bewaringsplicht was namelijk zonder onderscheid van toepassing op alle personen die elektronische communicatie gebruiken en op alle gegevens, met uitzondering van de inhoud van de gegevens.[285] Net zoals het Hof van Justitie had vastgesteld met betrekking tot de dataretentierichtlijn, was deze wet dus ook van toepassing op personen voor wie er geen enkele aanwijzing bestond dat hun gedrag – zelfs maar indirect of van ver – een verband vertoonde met de in de bestreden wet opgesomde inbreuken. Op dezelfde wijze voorzag de wet evenmin een uitzondering voor het bewaren van gegevens van beroepsgeheimhouders.[286] Vervolgens stelde het Hof vast dat bij de wet geen enkele materiële of procedurele voorwaarden werden vastgelegd met betrekking tot de toegang tot en het gebruik van bewaarde gegevens.[287] Er waren bijgevolg volgens het Hof onvoldoende waarborgen om misbruik tegen te gaan. Ook hekelde het Hof het gebrek aan een voorafgaande rechterlijke of onafhankelijke administratieve controle. Ten slotte stelde het Hof dat de wetgever de grenzen had overschreden die worden opgelegd door de eerbiediging van het evenredigheidsbeginsel in het licht van de artikelen 7, 8 en 52, lid 1, van het EU-Handvest, doordat de wet voor de bewaarperiode van de gegevens geen onderscheid maakte naargelang het nut, het doel of de betrokken personen.[288] Niettemin achtte het Hof de bewaring van gegevens op zich wel geschikt in de strijd tegen zware criminaliteit, maar stelde het vragen over de noodzakelijkheid van een algemene bewaringsplicht. Als gevolg van de vernietiging en het ontbreken van een handhaving van de vernietigde regeling, trad het oorspronkelijke artikel 126 WEC met de vage dataretentieplicht terug in werking.

73. **DATARETENTIEWET VAN 2016 –** Waar op Europees niveau aanwijzingen werden gegeven dat een nieuw wetgevend initiatief zou uitblijven, stelde de Belgische wetgever daarentegen redelijk snel een nieuwe dataretentiewet op.[289] Deze nieuwe wet beoogde tegemoet te komen aan de jurisprudentiële kritieken die zich situeerden op vier niveaus: (I) Het algemene karakter van de bewaringsplicht, (II) het gebrek aan differentiatie op grond van de categorieën van bewaarde gegevens en het nut ervan, (III) het gebrek aan of de ontoereikendheid van regels inzake de toegang van de overheden tot de betrokken gegevens en tot slot, hoewel dit element enkel wordt aangehaald door het Hof van Justitie, (IV) het gebrek aan of het tekortschieten van de regels inzake de beveiliging van de gegevens bij de aanbieders of de operatoren.[290] Belangrijk om te vermelden is dat de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna: Privacycommissie) een gunstig advies had gegeven met betrekking tot voorontwerp van de nieuwe dataretentiewet.[291] Zij gaf enkel de aanbevelingen om een samenwerkingsprotocol te

[284] C. CONINGS, "Dataretentieplicht en privacy" (noot onder GwH 11 juni 2015), *NJW* 2015, 911-913.
[285] GwH 11 juni 2015, nr. 84/2015, B.10.1.
[286] *Ibid.*
[287] GwH 11 juni 2015, nr. 84/2015, B.10.3.
[288] GwH 11 juni 2015, nr. 84/2015, overw. B.10.1-B.10.4, *NC* 2015, (486) 490-491, noot S. VERSTRAELEN.
[289] M. PANZAVOLTA, S. ROYER en H. SEVERIJNS, "Algemene dataretentie: ten minste houdbaar tot…?", *T.Strafr.* 2018*,* (3) 8.; Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *BS* 18 juli 2016, 44.717 (hierna Dataretentiewet van 2016)
[290] Wetsontwerp van 11 januari 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van elektronische communicatie, *Parl.St.* Kamer 2015-16, nr. 54-1567/001, 9-10.
[291] BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), *Adviesaanvraag inzake het voorontwerp van wet betreffende de bewaring van gegevens in de elektronische communicatiesector (CO-A-2015-040)*, 9

voorzien tussen het Instituut en de Privacycommissie om afdoende controle te garanderen, en om journalisten op te nemen in de uitzonderingsmaatregel voor bepaalde beroepsgroepen, ter bescherming van hun beroepsgeheim.[292] De aanbeveling met betrekking tot het samenwerkingsprotocol werd gevolgd[293], in tegenstelling tot de aanbeveling voor het opnemen van journalisten in de uitzonderingsmaatregel.[294] De Raad van State gaf daarentegen een langere lijst aan algemene en specifieke opmerkingen, waarvan een deel volgens de wetgever niet kon worden gevolgd. Deze hadden met name betrekking op: (I) kortere bewaartermijnen, met een activatie van langere termijnen in geval van een dreiging, (II) de reglementering van het verzoek gericht aan de operatoren, (III) de creatie van een specifieke database om art. 126 ten uitvoer te brengen en (IV) de controles en sancties in geval van niet-vernietiging van de data. Het advies werd op andere punten echter wel gevolgd.

74. Inhoudelijk wijzigde de dataretentiewet van 2016 de artikelen 46*bis*, 88*bis* en 90*decies* van het Wetboek van strafvordering, artikelen 2, 126, 126/1, 127 en 145 WEC en de artikelen 13, 18/3 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Ten eerste koppelde nieuw artikel 126, §2 WEC de toegang van elke instantie tot bewaarde gegevens aan concrete doelstellingen. Voor de gerechtelijke autoriteiten betekende dit dat in het kader van de strafprocedure ze enkel toegang hadden op basis van de artikelen 46*bis* en 88*bis* Sv. om misdrijven op te sporen, te onderzoeken en te vervolgen. Wat betreft de inlichtingendiensten, officieren van gerechtelijke politie, hulpdiensten, de Cel Vermiste Personen en de Ombudsdienst voor Telecommunicatie, hadden ze enkel toegang voor de specifieke doeleinden die binnen hun bevoegdheid vallen.[295] Ten tweede hernam de wet de algemene en ongedifferentieerde bewaarplicht van elektronische communicatiegegevens voor aanbieders van openbare telefoniediensten en operatoren van openbare elektronische communicatienetwerken in artikel 126 WEC. Er werd echter wel een onderscheid gemaakt tussen drie categorieën van gegevens: (I) identificatiegegevens, (II) verbindings- en lokalisatiegegevens en (III) persoonlijke communicatiegegevens.[296] Voor alle categorieën werd een bewaringstermijn van 12 maanden noodzakelijk geacht door de wetgever.[297] Uit de memorie van toelichting blijkt dat de wetgever een gerichte en gedifferentieerde bewaarplicht niet mogelijk heeft geacht en ervoor heeft gekozen om de algemene en ongedifferentieerde bewaarplicht met strikte waarborgen te omringen, zowel op het vlak van de beveiliging van de bewaring, als op het vlak van de toegang, zodat de inmenging in het recht op de bescherming van de persoonlijke levenssfeer tot een minimum zou worden beperkt.[298] In dit verband is erop gewezen dat een *a priori* differentiatie naar personen, periodes en geografische zones eenvoudigweg niet mogelijk zou zijn. Daarnaast

september 2015, nr. 33/2015, https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-33-2015.pdf.
[292] *Ibid,* 7 en 9.
[293] Art. 4, §4, 7°, tweede lid van de Dataretentiewet van 2016.
[294] *Ibid,* 108-110.
[295] M. PANZAVOLTA, S. ROYER en H. SEVERIJNS, "Algemene dataretentie: ten minste houdbaar tot…?", *T.Strafr.* 2018*,* (3) 8.
[296] Wetsontwerp van 11 januari 2016, *Parl.St.* Kamer 2015-16, nr. 54-1567/001, 13.
[297] C. FORGET, "L'obligation de conservation des "métadonnées": la fin d'une longue saga juridique?", *Journal des Tribunaux* 2017, (233) 235.
[298] Wetsontwerp van 11 januari 2016, *Parl.St.* Kamer 2015-16, nr. 54-1567/001, 10-13.

had de wetgever ook voorzien in een verscherping van de technische beveiligingsmaatregelen.[299] Zo moesten bijvoorbeeld de bewaarde gegevens vanaf hun registratie onleesbaar en onbruikbaar worden gemaakt voor elke persoon die niet gemachtigd is toegang te krijgen tot de gegevens. De gegevens moesten bovendien op het grondgebied van de Europese Unie worden bewaard en na de bewaringstermijn vernietigd worden. De niet-naleving van de voorschriften van artikel 126 WEC was strafbaar met een geldboete van € 50 tot € 50 000. Ten vierde kwam de wetgever tegemoet aan de kritiek van het Grondwettelijk Hof op het punt dat er geen materiële of procedurele voorwaarden aan de toegang tot de gegevens waren verbonden, door de procedures binnen de artikelen 46*bis* en 88*bis* Sv. te verstrengen.[300] De wetgever verstrengde ook de motiveringsplicht in artikel 88*bis* Sv. en er werd een trapsgewijs systeem ingesteld op basis van de ernst van het strafbare feit. Hoewel alle gegevens 12 maanden worden bewaard, kon de onderzoeksrechter ze niet tijdens die hele periode opvragen.[301] De maatregel kon niet bevolen worden voor misdrijven strafbaar met minder dan één jaar gevangenisstraf. Voor misdrijven strafbaar met één tot vijf jaren gevangenisstraf kon de aanvraag zes maanden teruggaan, voor misdrijven strafbaar met minstens vijf jaar gevangenisstraf of opgenomen in de lijst van artikel 90*ter* Sv. of gepleegd in het kader van een criminele organisatie, negen maanden en voor terroristische misdrijven 12 maanden.[302] Tot slot had de wetgever een regeling voor beroepsgeheimhouders uitgewerkt.[303] Deze regeling stelde dat de onderzoeksrechter slechts de communicatiegegevens van een advocaat of arts mag opvragen wanneer deze persoon zelf ervan wordt verdacht een feit strafbaar met een gevangenisstraf van minstens een jaar, te hebben gepleegd of aan zo'n strafbaar feit te hebben deelgenomen.[304] Bovendien kon de onderzoeksrechter de maatregel bevelen als precieze vermoedens bestaan dat derden de elektronische communicatiemiddelen van de beroepsgeheimhouder gebruiken en die derden verdacht worden van een feit strafbaar met een gevangenisstraf van minstens een jaar. De maatregel mocht niet ten uitvoer worden gelegd, zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte werd gebracht. Diezelfden werden door de onderzoeksrechter in kennis gesteld van hetgeen volgens hem onder het beroepsgeheim viel.[305] Deze gegevens werden niet opgenomen in het proces-verbaal.[306]

[299] M. PANZAVOLTA, S. ROYER en H. SEVERIJNS, "Algemene dataretentie: ten minste houdbaar tot…?", *T.Strafr.* 2018*,* (3) 9.
[300] Wetsontwerp van 11 januari 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van elektronische communicatie, *Parl.St.* Kamer 2015-16, nr. 54-1567/001, 14.
[301] M. PANZAVOLTA, S. ROYER en H. SEVERIJNS, "Algemene dataretentie: ten minste houdbaar tot…?", *T.Strafr.* 2018*,* (3) 9.
[302] Wetsontwerp van 11 januari 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van elektronische communicatie, *Parl.St.* Kamer 2015-16, nr. 54-1567/001, 40 ev.
[303] Oud art. 88*bis* Sv.
[304] *Ibid.*
[305] Wetsontwerp van 11 januari 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van elektronische communicatie, *Parl.St.* Kamer 2015-16, nr. 54-1567/001, 44.
[306] *Ibid.*

75. **GWH 19 JULI 2018, NR. 96/2018-** Vier beroepen werden ingesteld met het oog op de vernietiging van dataretentiewet van 2016. Het Grondwettelijk Hof moest zich, deze keer in navolging van het *Tele2*-arrest, voor een tweede keer uitspreken over de verenigbaarheid van een algemene bewaarplicht van telecommunicatiegegevens met de bescherming van persoonsgegevens en het privéleven.[307] Over het gehele arrest verwijst het Grondwettelijk Hof uitvoerig naar de rechtspraak van het Hof van Justitie. *Pro memorie* stelde het Hof van Justitie in het *Tele2*-arrest dat een nationale regeling die in geen enkele differentiatie, beperking of uitzondering naargelang van het nagestreefde doel voorziet, en die algemeen betrekking heeft op alle personen die gebruik maken van elektronischecommunicatiediensten, zonder geografisch onderscheid of onderscheid in de tijd, zonder dat rekening wordt gehouden met het feit dat die personen zich, al was het maar indirect, in een situatie bevinden die aanleiding kan geven tot strafvervolging of dat de communicatie van de gegevens betrekking heeft op personen van wie de communicaties onder het beroepsgeheim vallen, of zonder enig verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid te vereisen, de grenzen van het strikt noodzakelijke overschrijdt en niet kan worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is. Het Grondwettelijk Hof stelt daarbij vast dat de wetgever, met het aannemen van de bestreden wet, evenwel ruimere doelstellingen nastreeft dan de bestrijding van zware criminaliteit of het risico van een ernstige aantasting van de openbare veiligheid.[308] De regeling is ook van toepassing op alle personen zonder onderscheid, er wordt geen onderscheid gemaakt naargelang de periode, de geografische zone of een kring van personen.[309] Noch voorziet de regeling in een uitzondering voor de personen wiens communicaties onder het beroepsgeheim vallen. Het Grondwettelijk Hof merkt daarnaast ook op dat het merendeel van de lidstaten overigens grote moeilijkheden blijken te kennen om hun wetgeving inzake dataretentie in overeenstemming te brengen met de eisen die door het Hof van Justitie in zijn rechtspraak zijn gesteld.[310] Het besluit uiteindelijk dat bepaalde aspecten nog niet werden uitgeklaard door het Hof van Justitie waardoor het Hof nog niet kan oordelen over de voorliggende vragen. Alvorens ten gronde uitspraak te doen, werden drie prejudiciële vragen gesteld[311]: in de eerste plaats wordt de verenigbaarheid van de dataretentiewet met het Unierecht nagegaan. In het licht van de artikelen 7 en 8 van het EU-Handvest en het proportionaliteitsprincipe gewaarborgd door artikel 52, lid 1 EU-Handvest. Deze fundamentele rechten worden afgewogen tegen het recht op veiligheid, gewaarborgd door artikel 6 van het EU-Handvest. Ten tweede wordt de verenigbaarheid van de dataretentiewet met het Unierecht nagegaan in het bijzondere geval dat de algemene bewaarplicht wordt gebruikt om te voorzien in de effectieve identificatie en daadwerkelijke bestraffing van een dader van seksueel misbruik van minderjarigen. Het Grondwettelijk Hof wil dus nagaan of dit een legitieme doelstelling is waarvoor een inmenging in het recht op privacy is gerechtvaardigd. Ten derde gaat het Hof na of, in het geval van een vernietiging van de dataretentiewet, een tijdelijke doorwerking van de reeds ontstane rechtsgevolgen op basis van die wet mogelijk is.

[307] C. VAN DE HEYNING, "Overzicht van rechtspraak – Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog", *T.Strafr.* 2019, (38) 43.
[308] GwH 19 juli 2018, nr. 96/2018, B.3.3, B.3.4 en B.19.4.
[309] GwH 19 juli 2018, nr. 96/2018, B.20.2.
[310] *Ibid.*
[311] *Ibid.,* B.24.

76. **GWH 22 APRIL 2021, NR. 57/2021 -** Het Hof van Justitie heeft op de 3 prejudiciële vragen geantwoord met in het arrest *La Quadrature du Net e.a.* Uit dat arrest bleek dat het Unierecht zich verzet tegen wettelijke maatregelen die preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, behalve in bepaalde door het Hof van Justitie beschreven beperkte gevallen. De preventieve massale bewaring van gegevens is dus in beginsel strijdig met het Unierecht. Daarmee heeft het Hof van Justitie zijn vroegere rechtspraak bevestigd en tegelijkertijd de contouren gepreciseerd van de gevallen waarin de bewaring van gegevens is toegestaan. Het Hof van Justitie heeft voorts geoordeeld dat het Hof, in geval van vernietiging, de gevolgen van de bestreden wet niet kan handhaven omdat het anders het beginsel van de voorrang van het Unierecht op het nationale recht schendt.

Op grond van het arrest van het Hof van Justitie oordeelt het Grondwettelijk Hof dat de bestreden wet het Unierecht schendt, in zoverre zij principieel en zonder beperking tot de door het Hof van Justitie beschreven 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. Het Hof van Justitie wijst erop dat het Unierecht zich niet verzet tegen verschillende soorten wettelijke maatregelen die het Hof opsomt. Toelaatbaar zijn, 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 elektronischecommunicatiemiddelen ». De wettelijke maatregelen moeten echter wel duidelijke en nauwkeurige regels waarborgen dat aan de geldende materiële en procedurele voorwaarden wordt voldaan en voor zover de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik.[312] Het Hof stelt vast dat de bestreden wet berust op een verplichting tot algemene en ongedifferentieerde bewaring van alle gegevens met betrekking tot elektronische communicatie en dat zij ruimere doelstellingen nastreeft dan de bestrijding van zware criminaliteit of het risico van aantasting van de openbare veiligheid. Het onderscheid dat bij de bestreden wet wordt gemaakt tussen drie categorieën van gegevens (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 toegang tot die gegevens voor de gemachtigde instanties. Die categorisering stemt daarenboven niet overeen met het onderscheid dat door het Hof van Justitie wordt gemaakt, aangezien de bestreden wet noch de IP-adressen beoogt die zijn toegewezen aan de bron van een verbinding, noch de gegevens inzake de burgerlijke identiteit van de gebruikers.[313] De verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel. Er

[312] GwH 22 april 2021, nr. 57/2021, B.16.1.
[313] *Ibid.,* B.17.

dient te worden voorzien in duidelijke en nauwkeurige regels over de draagwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd, zodat wordt gewaarborgd dat de inmenging tot het strikt noodzakelijke wordt beperkt en dat zij evenredig is met het nagestreefde doel.[314]

Het Hof besluit daaruit dat het aan de wetgever staat een regeling tot stand te brengen waarbij de ter zake van toepassing zijnde beginselen in acht worden genomen, in het licht van de rechtspraak van het Hof van Justitie, en, waarbij ook, in voorkomend geval, rekening moet worden gehouden met de door dat Hof aangebrachte preciseringen wat betreft de verschillende soorten wettelijke maatregelen die met het Unierecht verenigbaar worden geacht. In het bijzonder staat het aan de wetgever tussen de verschillende soorten betrokken gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat, voor elk soort gegeven, de inmenging tot het strikt noodzakelijke wordt beperkt.[315] Het Hof vernietigt dus de bepalingen van de bestreden wet die de algemene en ongedifferentieerde bewaring betreffen van gegevens met betrekking tot elektronische communicatie en de toegang tot die gegevens. Gelet op het arrest van het Hof van Justitie oordeelt het Hof dat het de gevolgen van de vernietigde bepalingen niet voorlopig kan handhaven. Het Hof preciseert dat het aan de bevoegde strafrechter staat, in voorkomend geval, uitspraak te doen over de toelaatbaarheid van bewijzen die werden verzameld tijdens de inwerkingstelling van de vernietigde bepalingen, overeenkomstig de van toepassing zijnde strafprocedureregels en in het licht van de preciseringen van het Hof van Justitie in het voormelde arrest van 6 oktober 2020. Daaruit volgt dat de bewijzen die werden gehaald uit gegevens die zijn bewaard op grond van de vernietigde bepalingen veroordelingen kunnen verantwoorden, voor zover inzonderheid geen afbreuk wordt gedaan aan het recht van de betrokken personen op een eerlijk proces.

Na de vernietiging van de dataretentiewet van 2016 gold er geen algemene dataretentieverplichting. Echter mochten deze gegevens wel nog bijgehouden worden op basis van artikel 5 van de e-Privacy Richtlijn op basis van drie gronden: Dit geldt voor de gegevens die met toestemming van het data-subject werden bewaard, voor gegevens die worden bijgehouden voor de transmissie van de communicatie , en voor de gegevens die worden bijgehouden voor de facturatie, marketing of diensten met toegevoegde waarde.[316] Deze gegevens mogen alleen worden bewaard zolang als nodig voor de voorgeschreven doelstelling. Zoals het Hof van Justitie had geoordeeld, mochten de vervolgende instanties, rechterlijke instanties en inlichtingendiensten toegang hebben tot deze gegevens voor de bestrijding van criminaliteit, bescherming van de openbare orde en nationale veiligheid.[317]

[314] *Ibid.*, B.18.
[315] *Ibid.,* B.19.
[316] C. VAN DE HEYNING, "Het moeilijke evenwicht tussen privacy & veiligheid: De impact van het debat over bewaren van communicatiegegevens", *Radices* 2022, (132) 147.
[317] *Ibid.*

77. **DATARETENTIEWET VAN 2022 –** De wetgever werd voor een derde keer naar de tekentafel gestuurd om een nieuw juridisch kader uit te werken. Hoewel het Hof van Justitie en het Grondwettelijk Hof de Belgische wetgever voor een moeilijke opdracht plaatsten, liet een voorontwerp van de nieuwe dataretentiewet niet lang op zich wachten.[318] Zoals verwacht bleef het voorontwerp niet gespaard van kritiek. Stemmen gingen op dat de wetgever een brede invulling gaf aan de mogelijkheden voor gerichte bewaring en ook op het vlak van de toegang tot de bewaarde data niet veel beperkingen leek ingevoerd te hebben.[319] De nieuwe dataretentiewet werd uiteindelijk op 7 juli 2022 goedgekeurd door het Parlement. Deze wet moet nu tegemoetkomen aan de rechtspraak van het Hof van Justitie en het Grondwettelijk Hof inzake bewaring van de "metagegevens" of "verkeers- en locatiegegevens" door operatoren. De nieuwe wet beoogt ook te beantwoorden aan de legitieme maatschappelijke verwachtingen van een wereld die steeds digitaler wordt.[320] Om specifieke vormen van online overtredingen aan te pakken, is het nodig dat de autoriteiten die verantwoordelijk zijn voor de preventie, opsporing en vervolging van deze overtredingen, toegang hebben tot de gegevens kunnen die worden bewaard door de operatoren, in de mate dat dit noodzakelijk is om hun respectieve opdrachten uit te voeren.[321] De nieuwe dataretentiewet van 2022 zal ongetwijfeld niet het laatste hoofdstuk uit de dataretentiesaga zijn, aangezien er intussen maar liefst vijf vernietigingsberoepen bij het Grondwettelijk Hof zijn ingesteld.

[318] S. CAREEL en S. ROYER, "Voorontwerp dataretentiewet: derde keer, goede keer?", *DJK* 2021, 10.
[319] Zie bv. Gegevensbeschermingsautoriteit 28 juni 2021, adv. nr. 108/2021, 57-58.; S. CAREEL en S. ROYER, "Voorontwerp dataretentiewet: derde keer, goede keer?", *DJK* 2021, 10-11.
[320] Wetsontwerp van 17 maart 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, *Parl.St.* Kamer 2021-22, nr. 55-2572/001, 4.
[321] *Ibid.*

4.3. Analyse van de Belgische dataretentiewet van 2022

4.3.1. Personeel toepassingsgebied

78. **OPERATOREN –** Sinds de wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie[322] bestaat het "klassieke" onderscheid tussen netwerkoperatoren enerzijds en operatoren van elektronische-communicatiediensten anderzijds niet meer.[323] Netwerkoperatoren zijn bijvoorbeeld Telenet en Proximus. Voor operatoren van elektronische-communicatiediensten kan er het beste verwezen worden naar bijvoorbeeld Gmail, Netflix en Facebook/Meta. Artikel 2, 11° van de Telecomwet definieert nu operator als "een persoon of onderneming die een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische-communicatiedienst aanbiedt". De bewaarplicht geldt nu voor alle exploitanten, terwijl de vorige wetgeving vooral in België gevestigde netwerkexploitanten verplichtte om gegevens te bewaren.[324] Hoewel deze wijziging een aanzienlijke verruiming van het personeel toepassingsgebied van de gegevensbewaring lijkt in te houden, moet wel in het achterhoofd gehouden worden dat de te bewaren gegevens moeten "gegenereerd of verwerkt" zijn door de genoemde exploitanten. Verwerking houdt in dat een bewerking of een geheel van bewerkingen wordt gedaan met betrekking tot deze gegevens, bijvoorbeeld verzamelen, ordenen, opslaan, bewerken, raadplegen etc. Om het effect van deze beperking te illustreren, nam de minister van Justitie in het kader van de voorbereidende werkzaamheden het voorbeeld van de anonieme berichtendienst Signal.[325] Hij wees erop dat deze dienst volgens zijn voorwaarden alleen het voor de registratie gebruikte telefoonnummer bewaart, en dus verwerkt, en geen metadata genereert.[326] Volgens de minister hoeft Signal dus geen andere gegevens te bewaren dan het telefoonnummer dat de gebruiker vóór het gebruik van Signal heeft verstrekt**.**

4.3.2. Materieel toepassingsgebied

79. **SOORTEN GEGEVENS –** Eenvoudigweg onderscheiden we twee soorten gegevens die onderworpen zijn aan de bewaarplicht. Ten eerste zijn er identificatiegegevens. Dit zijn de gegevens die het mogelijk maken een gebruiker van een elektronische communicatiedienst te identificeren. Ten tweede zijn er verkeers- en locatiegegevens. *Ter herinnering:* verkeersgegevens zijn gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan, zoals gebelde nummers en de bijbehorende tijdstippen, alsook duur van de gevoerde gesprekken .[327] Locatiegegevens zijn ten slotte gegevens die worden verwerkt in een elektronische-communicatienetwerk waarmee de geografische positie van de eindapparatuur van een gebruiker

[322] Wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, *BS* 31 december 2021, 126491.
[323] B. FLUMIAN en V. FRANSSEN, Le droit pénal et la procédure pénale en constante évolution, Limal, Anthemis, 2022, 315-359.
[324] *Ibid*, 337.
[325] Rapport van de eerste lezing van 10 juni 2022, wetsontwerp nr. 55-2572/003, 72.
[326] *Ibid.*
[327] Art. 2, lid 2, b) e-privacy Richtlijn.

van een algemeen beschikbaar elektronische-communicatiedienst wordt aangegeven.[328] De verkeers- en locatiegegevens vallen nu onder de term "elektronische-communicatiemetagegevens", vervat in art. 2, lid 1, 93° van de Telecomwet. Deze terminologische wijziging loopt vooruit op de vervanging van de e-Privacy Richtlijn, waarin de term "verkeers- en locatiegegevens" wordt gebruikt. De toekomstige e-Privacy Verordening gebruikt onder artikel 4, lid 2, onder c), van het voorstel voor de e-Privacy Verordening de term "elektronische-communicatiegegevens".[329]

80. **KB VAN 19 SEPTEMBER 2013 –** De identificatiegegevens en elektronische-communicatiemetagegevens werden vóór de dataretentiewet van 2022 opgesomd in het Koninklijk Besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie.[330] Echter, in arrest nr. 158/2021 vernietigde het Grondwettelijk Hof artikel 2 van de wet van 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst", in zoverre het niet bepaalde welke identificatiegegevens werden verzameld en verwerkt en welke identificatiedocumenten in aanmerking kwamen.[331] Naar analogie heeft de wetgever de nieuwe dataretentiewet aangepast aan de uitspraak van het Grondwettelijk Hof en zowel de identificatiegegevens als de elektronische-communicatiemetagegevens expliciet vermeld in deze wet.[332] Een lijst van te bewaren gegevens is, gelet op de moeilijkheidsgraad, in vereenvoudigde vorm opgenomen in bijlages 2 en 3.

81. **IDENTIFICATIEGEGEVENS –** Wat betreft de identificatiegegevens, worden in artikel 126 WEC 17 identificatiegegevens opgesomd die door alle operatoren dienen bewaard te worden. Dit is een verbetering ten opzichte van de vorige regeling, in die zin dat de wet duidelijker en preciezer de identificatiegegevens omschrijft die moeten worden bewaard. Dit is in tegenstelling tot het KB van 19 september 2013, waar de te bewaren categorieën van gegevens werden opgesomd per categorie van operator, vaak in algemene bewoordingen. Wanneer de vergelijking wordt gemaakt tussen de identificatiegegevens opgenomen in het KB van 19 september 2013 en de identificatiegegevens opgesomd in artikel 126, §1 WEC, zijn deze gegevens echter min of meer identiek, behoudens bepaalde technologische ontwikkelingen sinds 2013.

82. De vraag die gesteld dient te worden is in welke mate deze identificatiegegevens overeenstemmen met de gegevens die zijn aangeduid door het Grondwettelijk Hof en het Hof van Justitie. Een verkeerde kwalificatie van een bepaald soort gegeven onder noemer van

[328] Art. 2, lid 2, c) e-Privacy Richtlijn.
[329] Voorstel (Comm.) voor een Verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie), 10 januari 2017, COM/2017/010 final - 2017/03 (COD).
[330] KB van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 8 oktober 2013, 70828.
[331] GwH 18 november 2021, nr. 158/2021.
[332] B. FLUMIAN en V. FRANSSEN, "Le nouveau cadre légal belge en matère de conservation des données de communications éléctroniques: " Old wine in new bottles" pour les autorités judiciaires? In A. MASSET e.a., *Le droit pénal et la procédure pénale en constante évolution,* Limal, Anthemis, 2022, (315) 334.

"identificatiegegevens" zou tot gevolg kunnen hebben dat de bewaring van en de toegang tot deze categorie niet in overeenstemming is met de vooropgestelde Europese criteria. De kwalificatie van het soort gegeven is bepalend voor zowel de doelstelling als het soort bewaarregime dat mag gehanteerd worden. Zoals duidelijk werd in de synthese, maakt het Hof van Justitie een onderscheid tussen burgerlijke identiteitsgegevens en IP-adressen die worden toegekend aan de bron van een verbinding. *Pro memorie*, voor de eerste groep van gegevens wordt een algemene bewaring niet problematisch geacht, voor de tweede groep van gegevens is een algemene bewaring slechts gerechtvaardigd in het kader van de bestrijding van ernstige criminaliteit, het voorkomen van ernstige bedreigingen van de openbare veiligheid en de bescherming van de nationale veiligheid. Zowel de Raad van State als de Gegevensbeschermingsautoriteit hadden erop gewezen dat het algemeen bewaren van aan de bron van een verbinding toegekende IP-adressen een ernstige inmenging inhoudt in de grondrechten die zijn verankerd in de artikelen 7 en 8 van het EU-Handvest en bijgevolg problematisch kan zijn in het licht van de rechtspraak van de hoogste rechtelijike instanties. De wetgever heeft hiermee rekening gehouden, aangezien de definitieve versie van artikel 127/1 WEC uitdrukkelijk bepaalt dat deze bewaarde IP-adressen enkel voor deze doeleinden mogen worden gebruikt wanneer ze het mogelijk maken de eindgebruiker te traceren. Dit is dan ook in overeenstemming met het Unierecht.

83. **ELEKTRONISCHE-COMMUNICATIEMETAGEGEVENS –** In artikel 126/2, §2 van de Telecomwet werden tien types van elektronische-communicatiemetagegevens opgenomen die dienen bewaard te worden door de operatoren. Dezelfde verbetering is te zien als bij de identificatiegegevens, in die zin dat de elektronische-communicatiemetagegevens duidelijker en preciezer omschreven worden. Ook dient opgemerkt te worden dat de lijst an de vroegere verkeers- en locatiegegevens in het koninklijk besluit van 19 september 2013 quasi identiek is aan de elektronische-communicatiemetagegevens opgenomen in de dataretentiewet, mits technologische revisie. Een lijst van te bewaren gegevens is in vereenvoudigde vorm opgenomen in bijlage 3 van de masterscriptie.

84. **AANPASSINGEN –** Zowel voor de gegevens in artikel 126 WEC als de gegevens in art. 126/2 WEC kan de Koning aanpassingen doorvoeren in het licht van de technologische ontwikkelingen. Het koninklijk besluit dat op deze basis wordt aangenomen, moet echter binnen zes maanden na de bekendmaking ervan bij wet worden bevestigd. Dit zou betrekking hebben op de hypothese dat, in het licht van de technologische ontwikkelingen, een nieuwe technologie ontstaat waarmee een persoon kan worden geïdentificeerd. Zo kan de Koning snel of zelfs proactief de gegevens die deze nieuwe norm vormt, kunnen laten behouden, maar hij zal ze moeten laten bevestigen door de wetgever. Ten slotte voorzien de artikelen 126 en 126/2 WEC ook in de mogelijkheid voor de Koning om, in voorkomend geval na het inwinnen van verschillende adviezen, de te bewaren gegevens te "specificeren" en "de vereisten inzake nauwkeurigheid en betrouwbaarheid vast te stellen waaraan deze gegevens moeten voldoen". Aangezien het doel is de kwaliteit van de te bewaren gegevens te verfijnen zonder de aard ervan te wijzigen, lijken deze bepalingen in overeenstemming met bovengenoemd arrest van het Grondwettelijk Hof van 18 november 2021.

4.3.3. Versleuteling

85. **ART. 107/5 WEC –** Het uittekenen van het encryptieverbod gebeurde niet zonder slag of stoot. Het basisprincipe in art. 107/5 WEC stelt nu dat het gebruik van versleuteling vrij is. Hierop heeft de wetgever echter drie beperkingen ingesteld, die als volgt kort kunnen worden samengevat: (i) het gebruik van versleuteling mag niet beletten dat een gebruiker de hulpdiensten kan bellen, noch dat de hulpdiensten de oproeper kunnen identificeren en localiseren, (ii) het gebruik van versleuteling, of de versleuteling nu end-to-end is of niet, mag niet tot gevolg hebben dat een operator niet kan voldoen aan haar verplichtingen inzake dataretentie en (iii) het gebruik van versleuteling door een buitenlandse operator mag niet tot gevolg hebben dat de operatoren, bij personen die een buitenlandse SIM kaart in hun toestel gebruiken op Belgisch grondgebied, als gevolg van deze versleuteling, niet meer kunnen voldoen aan de wettelijke bepalingen rond dataretentie en het onderscheppen van de inhoud van de communicatie.

86. **ACHTERDEUR –** De gegevensbeschermingsautoriteit had opgemerkt in zijn advies dat door van operatoren die een versleutelingssysteem opzetten te eisen dat zij rechtmatige interceptiemaatregelen mogelijk maken, het *de facto* de invoeging van "achterdeurtjes" in versleutelde systemen oplegt om de versleutelde berichten te kunnen ontcijferen.[333] Daarbij bestaat er sinds de jaren negentig in de wetenschappelijke gemeenschap een sterke consensus dat het inbouwen van "achterdeurtjes" in versleutelde systemen meer risico's inhoudt voor de privacy van de betrokken personen en voor de hogere belangen van staten dan dat het voordelen oplevert voor de bestrijding van zware criminaliteit. Daarbovenop verwijst de Autoriteit naar de verschillende middelen waarover de handhavingsautoriteiten reeds beschikken om om zware criminaliteit te bestrijden. De minister van justitie beantwoordde deze kritiek door te stellen dat elke bewaarplicht onzinnig wordt als deze gegevens niet meer leesbaar en dus niet meer beschikbaar zijn.[334] In een open brief van 107 organisaties en cybersecurity-experten wordt er gesteld dat er geen manier is om derden toegang te geven tot end-to-end versleutelde communicatie zonder ook encryptie-backdoors en kwetsbaarheden te creëren die kunnen worden uitgebuit door iedereen die ze vindt.[335] Het creëren van achterdeurtjes in encryptie verzwakt de veiligheid van het hele systeem en brengt alle gebruikers in gevaar.

87. **ENCRYPTIEDEBAT IN DE EU –** Hoewel het Hof van Justitie zich niet gebogen heeft over encryptiemaatregelen in de context van dataretentie, lijkt het wel aangewezen om dit debat op het niveau van de Europese Unie kort te schetsen. Binnen dit debat wordt encryptie op twee

[333] BESCHERMING VAN DE PERSOONLIJKE LEVENSFEER (CPBL), Adviesaanvraag 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 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 (CO-A-2021-099), 28 juni 2021, nr. 108/2021, https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-108-2021.pdf, overw. 162-163.
[334] Wetsontwerp van 17 maart 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**,** *Parl. St.* Kamer 2021-22, nr. 55-2572/001, 19.
[335] GLOBAL ENCRYPTION COALITION, "Open Letter: 107 organizations and cybersecurity experts call on the Belgian Government to halt legislation to undermine end-to-end encryption, 28 september 2021, www.globalencryption.org/2021/09/open-letter-48-organizations-and-cybersecurity-experts-call-on-the-belgian-government-to-halt-legislation-to-undermine-end-to-end-encryption/.

tegenstrijdige manieren gezien. Het is ten eerste een instrument voor privacy en veiligheid en daarom een essentieel onderdeel van open samenlevingen en markten, maar er wordt ook beweerd dat het een dekmantel is voor criminele activiteiten en daarom een obstakel voor wetshandhaving.[336] Pogingen om encryptie te verzwakken of te breken om criminaliteit te bestrijden, ondermijnen ook de Europese privacy en veiligheid. Op Europees niveau werd ondertussen in verschillende domeinen actie ondernomen om de balans te vinden tussen deze twee zienswijzen. Dit was bijvoorbeeld het geval met betrekking tot encryptie en gegevens over seksueel misbruik van kinderen.[337] Het beleid en de mogelijkheden inzake toegang tot gegevens verschillen echter van lidstaat tot lidstaat, waardoor de problemen met encryptie in strafrechtelijke onderzoeken van lidstaat tot lidstaat verschillen. Zoals de Europese Commissie in haar werkdocument uiteenzet, is er niet één technologische oplossing om rechtshandhaving toegang te verschaffen tot versleutelde gegevens, maar zijn er verschillende oplossingen met verschillende niveaus van effectiviteit, haalbaarheid, privacy, veiligheid en transparantie. Het Europees Comité voor gegevensbescherming (hierna: EDPB) is in het kader van de e-Privacy Verordening van mening dat het gebruik van end-to-end-encryptie moet worden aangemoedigd en, indien nodig, verplicht moet worden gesteld. In dit verband moeten maatregelen worden overwogen om de ontwikkeling van technische normen inzake encryptie aan te moedigen. De EDPB is van mening dat de e-Privacy Verordening specifiek moet verbieden dat aanbieders van encryptie, communicatiediensten en alle andere organisaties op alle niveaus van de toeleveringsketen "uitzonderlijke toegangssleutels" en "achterdeurtjes" toestaan of vergemakkelijken. Systemen met uitzonderlijke toegang tot sleutels of met achterdeurtjes kunnen de communicatie complexer en minder veilig maken. Bovendien kunnen backdoors worden gebruikt voor onwettige doeleinden en ook problematisch zijn met betrekking tot de GDPR, met name in verband met art. 5, 24, 28, 33 en 34 van de AVG.

88. **CONCLUSIE –** Deze bepaling zal in de toekomst zonder twijfel onder vuur liggen, gelet op de bescherming van het recht op privacy en persoonsgegevens en de komst van de e-Privacy Verordening.

[336] N. KOOMEN, "The Encryption Debate in the European Union: 2021 Update", *Carnegie Endowment for International Peace* 2021, 2-3.
[337] *Ibid.*

4.3.4. Bewaringsregimes

4.3.4.1. Algemene bewaring

89. **ALGEMEEN –** De nieuwe dataretentiewet introduceert drie regelingen die voorzien in een algemene en ongedifferentieerde bewaring. Deze zitten vervat in art. 126, §1 WEC voor identificatiegegevens, art. 126/3, §2, lid 2 WEC voor de identificatiegegevens en elektronische-communicatiemetagegevens (verkeers- en locatiegegevens) en art. 13/7 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, ook voor de identificatiegegevens en elektronische-communicatiemetagegevens (verkeers- en locatiegegevens).

90. **Art. 126 WEC** – Art. 126, §1 WEC stelt dat onverminderd de AVG en de wet van 30 juli 2018, 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 identificatiegegevens opgenomen in bijlage 2 van de masterscriptie bewaren, voor zover ze die verwerken of genereren in het kader van de verstrekking van die netwerken of diensten. Zoals blijkt uit de rechtspraak van het Hof van Justitie verschaffen deze gegevens, afgezien van de contactgegevens van de betrokken gebruikers, geen communicatiegegevens en dus geen informatie over hun privéleven. De inmenging die de bewaring van die gegevens met zich meebrengt is dus geen ernstige inmenging in de rechten van de burgers. Hieruit volgt dat wettelijke maatregelen die betrekking hebben op de verwerking van die gegevens als zodanig, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van de e-Privacy Richtlijn genoemde doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen.

De bewaring van de identificatiegegevens strookt met de voorwaarden opgesteld door het Hof van Justitie. Het bewaren van de identificatiegegevens zijn uitsluitend gericht op de identificatie van de betrokken gebruiken en worden niet in verband worden gebracht met informatie over de gedane mededelingen. Deze visie wordt ook gesteund door VAN ROY en ROYER, stellende dat een algemene bewaring van deze gegevens toegestaan is omdat ze niet toelaten om concrete informatie over de communicatie te verkrijgen.

91. **Art. 126/3, §2, tweede lid WEC –** Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse (hierna: OCAD) 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 WEC over te gaan voor het gehele grondgebied. De bewaarplicht moet bevestigd worden 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 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. Zoals blijkt uit de synthese in hoofdstuk 3, heeft het Hof van Justitie drie voorwaarden gesteld opdat een algemene en ongedifferentieerde verzameling van verkeers- en locatiegegevens gerechtvaardigd is. De eerste voorwaarde is dat er voldoende concrete aanwijzingen moeten zijn dat de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging voor de nationale veiligheid die reëel en actueel of voorzienbaar is. De tweede voorwaarde is dat het bevel zonder onderscheid alle gebruikers van elektronische communicatie kan treffen, maar moet beperkt zijn in de tijd (hoewel verlenging mogelijk is). Tenslotte is de derde voorwaarde dat het bevel tot bewaring moet worden onderworpen zijn aan effectieve toetsing, hetzij door een rechtbank, hetzij door een onafhankelijke administratieve instantie waarvan de beslissing bindend is, waarbij de toetsing tot doel heeft na te gaan of een van deze situaties zich voordoet en of de voorwaarden en waarborgen die moeten worden gesteld, in acht worden genomen. In de volgende randnummers wordt de overeenstemming van deze bewaarplicht met de drie voorwaarden één voor één besproken.

92. **ERNSTIGE BEDREIGING VAN DE NATIONALE VEILIGHEID –** Met betrekking tot de eerste voorwaarde moet er verwezen worden naar de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna: wet inlichtingendiensten), de wet van 10 juli 2006 betreffende de analyse van de dreiging en het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging. De keuze van het dreigingsniveau van OCAD als bewaringscriterium werd met name gerechtvaardigd door het feit dat dit orgaan volledig onafhankelijk is van zowel de operatoren die de gegevens bewaren als van de diensten of autoriteiten die toegang tot deze gegevens zouden kunnen vragen. Artikel 8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten definieert het begrip "activiteit die bedreigt of zou kunnen bedreigen" als elke individuele of collectieve activiteit ontplooid in het land of vanuit het buitenland die verband kan houden met spionage, inmenging, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties, criminele organisaties, daarbij inbegrepen de verspreiding van propaganda, de aanmoediging of de rechtstreekse of onrechtstreekse steun, onder meer door het verstrekken van financiële, technische of logistieke middelen, het verstrekken van informatie over mogelijke doelwitten, de ontwikkeling van structuren en van actiecapaciteit en de verwezenlijking van denagestreefde doeleinden.

Het OCAD heeft vier opdrachten. Ten eerste voert het OCAD op periodieke basis een gemeenschappelijke strategische evaluatie uit die moet toelaten te oordelen of dreigingen zich kunnen voordoen of, indien ze al vastgesteld werden, hoe deze evolueren en welke maatregelen in voorkomend geval noodzakelijk zijn. De tweede opdracht is op punctuele basis een gemeenschappelijke evaluatie uitvoeren die moet toelaten te oordelen of dreigingen zich voordoen en welke maatregelen in voorkomend geval noodzakelijk zijn. De derde taak bestaat uit contacten verzekeren met gelijkaardige buitenlandse of internationale diensten specifieke internationale. Ten slotte heeft de vierde opdracht betrekking op het coördineren van de globale aanpak tegen dreigingen. Iedere evaluatie zal het niveau van de dreiging bepalen door zich te

steunen op een beschrijving van de ernst en de waarschijnlijkheid van het gevaar of van de dreiging. Wanneer het dreigingsniveau "Niveau 3 of ERNSTIG" bereikt, blijkt dat de dreiging tegen de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse mogelijk en waarschijnlijk is. Bij het "Niveau 4 of ZEER ERNSTIG" blijkt dat de dreiging tegen de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse ernstig en zeer nabij is. De Belgische wet lijkt te voldoen aan de eerste voorwaarde, omdat de toepassing van de algemene en ongedifferentieerde bewaring afhankelijk wordt gemaakt van dreigingsniveau 3 of hoger van het OCAD. Gelet op het voorgaande, kan er dus worden aangenomen dat de bewaarplicht redelijkerwijs wordt gekoppeld aan een ernstige bedreiging voor de nationale veiligheid die reëel en actueel of voorzienbaar is.

93. **ONAFHANKELIJKHEID OCAD MOGELIJK IN GEDRANG–** OCAD is een orgaan belast met de evaluatie van de dreigingen die de inwendige en uitwendige veiligheid van de Staat, de Belgische belangen en de veiligheid van de Belgische onderdanen in het buitenland of elk ander fundamenteel belang van het land zoals bepaald door de Koning op voorstel van de Nationale Veiligheidsraad, zouden kunnen aantasten.[338] OCAD staat onder het gemeenschappelijke gezag van de minister van Justitie en de minister van Binnenlandse Zaken en valt onder het toezicht van onafhankelijke Comités P en R .[339] Een van de beweegredenen om de algemene retentie te koppelen aan de dreigingsanalyse door het OCAD is omwille van de onafhankelijkheid van de instelling. Volgens een letterlijke lezing van art. 126/3, §2, lid 2 WEC betekent een dreigingsniveau van ten minste niveau drie automatisch een algemene en ongedifferentieerde bewaring van de gegevens bedoeld in artikel 126/2, § 2 WEC over het gehele grondgebied. Dit levert echter een probleem op met betrekking tot deze onafhankelijkheid van het OCAD. De onafhankelijkheid van het OCAD is namelijk niet alleen onafhankelijkheid van de politieke autoriteiten, maar ook een intellectuele onafhankelijkheid die OCAD in staat stelt de dreiging te beoordelen en een niveau vast te stellen dat uitsluitend gebaseerd is op zijn beoordelingstaak. De wet van 10 juli 2006 betreffende de dreigingsanalyse maakt een duidelijk onderscheid tussen het analysewerk van het OCAD en de overheidsinstanties die verantwoordelijk zijn voor de veiligheidsmaatregelen. Deze bepaling lijkt een nieuwe bevoegdheid aan OCAD te verlenen, dat nu kan "beslissen" over het bewaren van (gevoelige) gegevens op het gebied van elektronische communicatie. Dit nieuwe prerogatief kan OCAD in gevaar brengen bij het nemen van maatregelen die de wet OCAD had moeten voorkomen. De bewaarplicht moet namelijk worden bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. De bevestiging bij KB maakt dat de beslissing tot verplichte bewaring van de betrokken gegevens nog steeds een bestuurshandeling uitmaakt en dus blijft de afdeling Bestuursrechtspraak van de Raad van State ten volle bevoegd als annulatie- of schorsingsrechter ten aanzien van het KB. Een positief verhaal bij de Raad van State zou mogelijk de vraag kunnen oproepen of de vernietiging van het KB ook inhoudt dat als gevolg hiervan het OCAD het dreigingsniveau moet aanpassen. Dit zou dus rechtstreeks ingaan tegen de

[338] Art. 3 en 5 wet van 10 juli 2006 betreffende de analyse.
[339] Art. 5 wet van 10 juli 2006 betreffende de analyse.

onafhankelijkheidswaarborg. Voor de volledigheid dient wel vernoemd te worden dat de Raad van State de gevolgen kan handhaven.

94. **BEPERKT IN TIJD –** De bewaring zou beperkt moeten zijn in de tijd tot wat strikt noodzakelijk is en zou enkel opgelegd moeten worden voor een voorzienbare periode. Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. In het licht hiervan kan art. 126/3, §2 lid 2 en 3 WEC tekortkomen op twee vlakken, enerzijds op het vlak van de duur van de maatregel en anderzijds op het vlak van de verlenging van de maatregel. Met betrekking tot de duur valt op dat de wet niet vermeldt dat dergelijke maatregel beperkt dient te worden tot het strikt noodzakelijke. Daarbovenop geldt dat wanneer de beslissing tot algemene bewaring is genomen, deze bij koninklijk besluit dient te worden bevestigd. Dat koninklijk besluit bepaalt meteen ook de periode waarin de bewaarplicht geldt. Als er geen KB komt binnen een maand na het nemen van de beslissing, moet de bewaarplicht worden opgeheven.[340] Dat betekent dat een maatregel tot algemene bewaring geldt voor een periode van minstens een maand zonder dat een effectieve controle volgt. Ten slotte wat betreft de verlenging, dient te worden opgemerkt dat uit de lezing van de wet blijkt dat het aantal verlengingen niet beperkt wordt. Dit betekent dat aan de tweede voorwaarde niet voldaan is, aangezien de bewaring op deze manier niet beperkt blijft tot het strikt noodzakelijke.

95. **EFFECTIEVE TOETSING –** Ten derde moet er een effectieve toetsing zijn hetzij door een rechtbank, hetzij door een onafhankelijke administratieve instantie waarvan de beslissing bindend is. Van een effectieve toetsing was er geen sprake in de memorie van toelichting. De Raad van State rees in zijn advies de vraag op welke manier voldaan zou worden aan het vereiste van de "effectieve toetsing" in de zin van de rechtspraak van het Hof van Justitie. De ontworpen tekst moest in het licht van deze opmerking herzien en aangevuld worden. De wetgever heeft geen rekening gehouden met de opmerking van de Raad van State. De telecomwet bepaalt niet welke rechterlijke instantie of onafhankelijke bestuurlijke autoriteit op die beslissing toezicht uitoefent. Om te kunnen stellen dat er sprake is van een geldige algemene en ongedifferentieerde bewaarplicht ter waarborging van de nationale veiligheid, is het van groot belang dat aan de derde voorwaarde voldaan wordt. Hieruit blijkt dat deze voorwaarde niet vervuld is.

96. **CONCLUSIE –** Hoewel aan de eerste voorwaarde voldaan is, rijzen er vragen over de verenigbaarheid van de Belgische omzetting van de tweede en derde voorwaarde met de Unierechtelijke voorwaarden. Doordat het KB de periode bepaalt waarin de maatregel geldt en niet de wet zelf, bevat de regeling in de wet geen duidelijke en nauwkeurige regels over de

[340] Art. 126/3,§ 2, derde lid WEC.

reikwijdte en de toepassing van de betrokken maatregel. Daarnaast wordt er door de telecomwet geen effectieve toetsing ingevoerd hetzij door een rechtbank, hetzij door een onafhankelijke administratieve instantie waarvan de beslissing bindend is. Dit is nochtans een noodzakelijke voorwaarde opgesteld door het Hof van Justitie.

97. **ART. 13/7 WET INLICHTINGENDIENSTEN –** De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten en in geval van een reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, de medewerking vorderen van de operatoren van een elektronisch communicatienetwerk en de verstrekkers van een elektronische communicatiedienst om over te gaan tot de algemene en ongedifferentieerde bewaring van de door hen gegenereerde en verwerkte elektronische-communicatiemetagegevens (verkeers- en lokalisatiegegevens) van elektronische communicatiemiddelen. Deze vordering kan enkel ingesteld worden mits een voorafgaand schriftelijk akkoord van de BIM-commissie. De commissie geeft haar akkoord binnen vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd. Ook hier gelden dezelfde drie voorwaarden opgesteld door het Hof van Justitie als vermeld in de synthese en in randnummer 91. Ten eerste moeten er voldoende concrete aanwijzingen zijn dat de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging voor de nationale veiligheid die reëel en actueel of voorzienbaar is. Ten tweede moet het bevel beperkt zijn in de tijd (hoewel verlenging mogelijk is). Tenslotte moet het bevel tot bewaring onderworpen zijn aan effectieve toetsing, hetzij door een rechtbank, hetzij door een onafhankelijke administratieve instantie waarvan de beslissing bindend is, waarbij de toetsing tot doel heeft na te gaan of een van deze situaties zich voordoet en of de voorwaarden en waarborgen die moeten worden gesteld, in acht worden genomen.

98. **ERNSTIGE BEDREIGING VAN NATIONALE VEILIGHEID** – In België zijn er twee inlichtingen- en veiligheidsdiensten, namelijk De Veiligheid van de Staat als burgerlijke inlichtingendienst en de Algemene Dienst Inlichting en Veiligheid als militaire inlichtingendienst. De voornaamste taak van De Veiligheid van de Staat bestaat in het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel of elk ander fundamenteel belang van het land bedreigt of zou kunnen bedreigen. Ze voeren veiligheidsonderzoeken uit die haar worden toevertrouwd. De Algemene Dienst Inlichting en Veiligheid heeft als voornaamste taak het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, alsook de inlichtingen die betrekking hebben op militaire activiteiten. Zoals reeds aangehaald in randnummer 97, kan deze vordering enkel ingesteld worden mits een voorafgaand schriftelijk akkoord van de BIM-commissie. In art. 13/7, §3 van de wet inlichtingendiensten wordt een opsomming gegeven van de vermeldingen die de vraag van het diensthoofd om een vordering tot bewaring in te stellen moet bevatten, op straffe van onwettigheid. Deze omvatten onder

andere de ernstige dreiging tegen de nationale veiligheid die reëel en actueel of voorzienbaar is (1°) alsook de feitelijke omstandigheden die de ongedifferentieerde en algemene bewaring van de verkeers- en lokalisatiegegevens rechtvaardigen (2°). Daarnaast moet de inlichtingen- en veiligheidsdienst om de twee weken verslag uitbrengen aan de commissie over de evolutie van de dreiging. Dit verslag belicht de elementen die ofwel de handhaving van de algemene en ongedifferentieerde bewaring, ofwel de beëindiging ervan, rechtvaardigen. Gelet op het voorgaande en aangezien de inlichtingen- en veiligheidsdiensten verantwoordelijk zijn voor de beoordeling van deze dreigingen, kan worden aangenomen dat aan de voorwaarde van een ernstige bedreiging voor de nationale veiligheid die reëel en actueel of voorzienbaar redelijkerwijs voldaan is.

99. **BEPERKT IN TIJD –** Vervolgens moet de bewaring beperkt zijn in de tijd tot wat strikt noodzakelijk is. Wanneer er gekeken wordt naar art. 13/7, §3, 4° van de wet inlichtingendiensten, moet op straffe van onwettigheid de vraag van het diensthoofd om een vordering tot bewaring in te stellen de duur van de bewaringsmaatregel vermelden. Die duur mag niet langer zijn dan zes maanden, te rekenen vanaf de datum van de vordering. Hij kan volgens dezelfde procedure wel worden verlengd. In tegenstelling tot art. 126/3, §2, tweede lid WEC vermeldt deze bepaling wel een maximumtermijn. Het diensthoofd moet ook de vordering beëindigen, niettegenstaande de bevestiging bij koninklijk besluit, wanneer de bewaring niet langer van nut is voor de bestrijding van de reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, wanneer deze dreiging is verdwenen of wanneer hij een onwettigheid vaststelt. Op basis van deze elementen lijkt het dat aan deze voorwaarde voldaan is door de Belgische wetgever.

100. **EFFECTIEVE TOETSING –** De derde voorwaarde vereist dat er een effectieve toetsing gebeurt hetzij door een rechtbank, hetzij door een een onafhankelijke administratieve instantie waarvan de beslissing bindend is. De BIM-commissie is een bestuurlijke commissie dat het voorafgaand akkoord moet geven voor de vordering tot bewaring. De commissie is samengesteld uit drie effectieve leden en handelt volledig onafhankelijk in de uitoefening van haar controleopdrachten. De effectieve leden en hun plaatsvervangers hebben de hoedanigheid van magistraat. Onder de effectieve leden heeft één lid de hoedanigheid van lid van het openbaar ministerie en hebben beide anderen de hoedanigheid van rechter, waarvan één deze van onderzoeksrechter. De Commissie beslist bij meerderheid van de drie aanwezige effectieve leden of van hun plaatsvervanger of, in geval van verhindering van een van de effectieve leden en diens plaatsvervanger, bij unanimiteit van de twee aanwezige effectieve leden of van hun plaatsvervanger. In geval van hoogdringendheid vraagt het diensthoofd vooraf om het mondelinge akkoord van de voorzitter van de commissie of, indien deze niet beschikbaar is, een ander lid van de commissie. De auteur van het akkoord informeert onmiddellijk de andere commissieleden. Het diensthoofd bevestigt zijn vraag schriftelijk binnen vierentwintig uur volgend op het akkoord. De voorzitter of het gecontacteerde lid bevestigt eveneens zo spoedig mogelijk schriftelijk zijn akkoord. Dit akkoord is gedurende vijf dagen geldig. De controle *ex post* bestaat opnieuw uit een bevestiging bij koninklijk besluit binnen een maand na de vordering.

Ondanks dat er normaliter toch een controle e*x post* mogelijk zou moeten zijn op basis van het gemeenrecht, kan er wel gesteld worden dat er een duidelijke voorafgaande effectieve toetsing gebeurt door een onafhankelijke administratieve instantie. Deze beslissing is ook bindend, aangezien de BIM-commissie binnen de vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd bepaalt of de vordering tot bewaring wettig is of niet. *Ex ante* controle kan met andere woorden volstaan onder de rechtspraak van het Hof van Justitie. Als er geen *ex ante* controle is, maakt het de mogelijkheid tot *ex post* rechterlijke toetsing des te belangrijker. In conclusie lijkt dus aan deze derde voorwaarde ook voldaan te zijn.

101. **CONCLUSIE –** Uit het voorgaande kan geconcludeerd worden dat de drie voorwaarden opgesteld door het Hof van Justitie lijken vervuld te zijn. De regeling is in deze hoedanigheid in overeenstemming met het Unierecht.

4.3.4.2. Gerichte bewaring

102. **ALGEMEEN –** Artikel 126/1, §1 WEC vormt de wettelijke basis voor een gerichte bewaring op basis van geografische criteria. Het artikel stelt dat de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die onderliggende en elektronische-communicatienetwerken aanbieden, de elektronische-communicatiemetagegevens in artikel 126/2, § 2 voor de geografische zones bedoeld in artikel 126/3, gedurende twaalf maanden te rekenen vanaf de datum van de communicatie bewaren, tenzij een andere termijn bepaald is in artikel 126/3. Zoals blijkt uit de synthese in hoofdstuk 3 heeft het Hof van Justitie voor een gerichte bewaring van verkeers- en locatiegegevens drie voorwaarden uitgewerkt. Ten eerste moet de doelstelling bestaan in het bestrijden van ernstige criminaliteit en/of het voorkomen van ernstige bedreigingen van de openbare veiligheid inhoudt. Ten tweede moet de gerichte bewaring worden beperkt op basis van objectieve en niet-discriminerende factoren. Ten derde mag de duurtijd van de bewaring niet langer zijn dan strikt noodzakelijk in het licht van het nagestreefde doel en de omstandigheden die deze rechtvaardigen, onverminderd de mogelijkheid om deze maatregelen te verlengen indien de bewaring noodzakelijk blijft.

103. **DOELSTELLING –** Art. 126/1, §1 derde lid WEC stelt dat deze gegevens worden bewaard ten behoeve van vier doelstellingen, met name: (I) De vrijwaring van de nationale veiligheid, (II) de strijd tegen zware criminaliteit, (III) de preventie van ernstige dreigingen van de openbare veiligheid, en (IV) de bescherming van de vitale belangen van een natuurlijke persoon. De eerste drie doelstellingen sluiten aan bij de toegelaten doelstellingen opgesomd door het Hof van Justitie. De vierde doelstelling komt niet voor in de rechtspraak van het Hof. Dit werd ook opgemerkt door de Raad van State in zijn advies 69.381/4 van 28 juni 2021. Het stelde namelijk dat het "deel uitmaakt van een andere context dan die van de prejudiciële vragen waarop het Hof van Justitie geantwoord heeft in zijn arrest *La Quadrature du Net*", en dat "een dergelijk doeleinde hoe dan ook *a priori* geacht kan worden te vallen onder de bescherming van de openbare veiligheid en onder de positieve verplichtingen die in dat verband op de lidstaten rusten ter bescherming van het leven en de veiligheid van personen". In de memorie van toelichting wordt verduidelijkt dat deze doeleinde overeenstemt overeen met dat van artikel 6.1, d) van de AVG.[341] De wetgever geeft daarnaast ook nog twee voorbeelden in de praktijk waarin de vitale belangen van de persoon centraal staan: het gebruik van locatiegegevens door de cel Vermiste Personen van de federale politie en door de nooddiensten die ter plaatse hulp bieden. VAN ROY en ROYER geven nog twee mogelijke verklaringen voor het opnemen van deze vierde doelstelling.[342] Zij stellen ten eerste dat het mogelijk is dat de wetgever de bescherming van de vitale belangen van de persoon aanhaalt om te wijzen op zijn positieve mensenrechtelijke verplichtingen als extra argument voor de gerichte bewaring. Ten tweede halen ze aan dat de wetgever mogelijk dezelfde logica als voor artikel 127/1, § 2, 3° WEC betreffende de toegang tot de gegevens zou volgen. Hier verduidelijkte hij wel waarom de vitale belangen van de persoon

[341] "De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen".
[342] L. VAN ROY, L. en S. ROYER, "De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep", *NC* 2023, (1) 14.

in het artikel terechtkwamen. Hieruit volgt dat aan deze voorwaarde voldaan is door de Belgische wetgever.

104. **OBJECTIEVE EN NIET-DISCRIMINERENDE FACTOREN –** Het Hof van Justitie gaf zelf aanwijzingen op welke manier de gerichte bewaring op basis van objectieve en niet-discriminerende factoren kon bereikt worden. Zo zei het Hof dat de beperkingen kunnen worden vastgesteld volgens de categorieën van betrokken personen op basis van objectief bewijsmateriaal dat het mogelijk maakt zich te richten op personen wier verkeers- en locatiegegevens waarschijnlijk een verband, althans een indirect verband, met ernstige strafbare feiten aan het licht zullen brengen; of aan de hand van een geografisch criterium dat is vastgesteld op basis van objectieve en niet-discriminerende factoren (gebieden kunnen plaatsen omvatten waar veel ernstige criminaliteit voorkomt, plaatsen die bijzonder kwetsbaar zijn voor het plegen van ernstige strafbare feiten, zoals plaatsen of infrastructuur die regelmatig een zeer groot aantal bezoekers ontvangen, of strategische locaties, zoals luchthavens, stations…). Er worden verschillende criteria gebruikt door de Belgische wetgever om de geografische zone af te bakenen. Ten eerste is er het statistisch criterium van "ernstige criminaliteit", ten tweede is er het criterium van "dreiging" en ten slotte zijn er drie categorieën van 'strategische' geografische zones.

105. **GEOGRAFISCHE ZONES O.B.V. ERNSTIGE CRIMINALITEIT –** De wetgever heeft dus allereerst de geografische gebieden afgebakend waarop het statistische criterium moet worden toegepast, namelijk de gerechtelijke arrondissementen en subsidiair, de politiezones. De drempel voor ernstige misdrijven is vastgesteld op drie strafbare feiten in de zin van artikel 90*ter*, paragrafen 2 tot en met 4 van het Wetboek van strafvordering (hierna: Sv.) per 1.000 inwoners, vastgesteld over een gemiddelde van de voorbije drie kalenderjaren.

106. **ERNSTIGE CRIMINALITEIT –** De wetgever is van mening dat het gebruik van het aantal feiten die momenteel als de meest ernstige worden beschouwd, een goede indicator is voor het bepalen van de zones met een hoge criminaliteit. In feite is het gebruik van deze lijst van artikel 90*ter*, §§ 2 tot en met 4 alleen bedoeld als een indicator voor het bepalen van gebieden met een hoog aantal feiten van zware criminaliteit. Hoewel de lijst de strafbare feiten bevat die over het algemeen als de ernstigste worden beschouwd, sluit dit niet uit dat ook strafbare feiten buiten deze lijst kunnen worden geacht een voldoende mate van ernst te hebben in verhouding tot de door deze gegevensbewaring teweeggebrachte inmenging. Zoals bleek uit het *arrest Ministerio Fiscal* hanteert het Hof van Justitie ook geen definitie van "zware criminaliteit".

In dit verband dient er ten eerste opgemerkt te worden dat over het gebruik van deze lijst als criterium onduidelijkheid heerst. Het valt namelijk niet af te leiden of artikel 90*ter*, §§ 2 tot 4 Sv. als lijst enkel ernstige misdrijven opsomt of hieronder ook misdrijven vallen die de nationale of openbare veiligheid bedreigen. Op basis van de lezing van de memorie van toelichting lijkt het enkel over ernstige misdrijven te gaan. Daarnaast heeft de wetgever ervoor gekozen noch een definitie van het begrip ernstige criminaliteit op te nemen, noch kernelementen aan te geven die wijzen op het 'ernstig' zijn van andere criminele gedragingen buiten de lijst. Er wordt namelijk

enkel verwezen naar deze lijst die als niet-exhaustief moet worden beschouwd. Hoewel zware criminaliteit als een dynamisch en evolutief begrip kan worden beschouwd, sluit dit niet uit dat het een mogelijkheid kan openen tot misbruik, of op zijn minst tot een bepaalde mate aan rechtsonzekerheid. Ten slotte kunnen er vragen gesteld worden bij de kwalificatie van bepaalde misdrijven opgesomd in de lijst. Bijvoorbeeld private omkoping (art. 504*bis* en 504*ter* Sw.), heling (art. 90*ter*, § 2, 29° Sv.) en informaticabedrog (art. 90*ter*, § 2, 28° Sv.) lijken moeilijk te plaatsen onder de noemer 'ernstige criminaliteit, laat staan onder de noemer 'nationale veiligheid of openbare veiligheid'. In het licht van het voorgaande lijken deze punten moeilijk verzoenbaar met de Europese dataretentierechtspraak.

107. **STATISTISCHE MOEILIJKHEDEN –** De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4 Sv. per jaar per 1.000 inwoners vastgesteld over een gemiddelde van de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank. 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. De wetgever stelt in de memorie van toelichting dat deze drempel voor zware criminaliteit, berekend per 1.000 inwoners, het mogelijk maakt rekening te houden met de objectieve realiteit van de criminele fenomenen binnen elk arrondissement, en tegelijkertijd de gelijke behandeling van de gehele bevolking te waarborgen. Bovendien staat dit statistisch criterium toe pieken en dalen in de criminaliteit die aan tijdelijke fenomenen te wijten zouden zijn uit te vlakken en laat het dus toe om de drempel te objectiveren. De referentieperiode van 3 jaar maakt het mogelijk voldoende betekenisvolle statistieken op te stellen en tegelijkertijd een actueel beeld van de criminaliteitscijfers te geven.

De gegevensbeschermingsautoriteit gaf in zijn advies aan dat de wetgever er op moet toezien dat de impact van deze drempel in de praktijk evenredig is met de huidige statistieken en spoort de wetgever tegelijkertijd aan een strenge en kwantitatieve analyse te maken van de evenredigheid van het criterium.[343] VAN DE HEYNING haalt correct aan dat de huidige regeling kan botsen met het doeltreffendheidsprincipe in die zin dat er een gebrek aan transparantie is op de impact van deze regeling op retentie en dus de beperking van de fundamentele rechten.[344] De beoordeling gebeurt namelijk op basis van de Algemene Nationale Gegevensbank, maar het is onduidelijk wanneer er sprake is van een "vastgesteld' misdrijf, namelijk vanaf een melding of klacht, wanneer er verdere vervolging is, of wanneer er ook een veroordeling of een alternatieve maatregel wordt opgelegd. In dit verband kan nog eens terugverwezen worden naar het advies van de gegevensbeschermingsautoriteit, die benadrukte dat het passender zou zijn om een

[343] BESCHERMING VAN DE PERSOONLIJKE LEVENSFEER (CPBL), Adviesaanvraag 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 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 (CO-A-2021-099), 28 juni 2021, nr. 108/2021, https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-108-2021.pdf, overw. 122.
[344] C. VAN DE HEYNING, "Het moeilijke evenwicht tussen privacy & veiligheid: De impact van het debat over bewaren van communicatiegegevens", *Radices* 2022, (132) 149.

databank te gebruiken waarvan de kwaliteit van de statistische gegevens is vastgelegd bij wet en om rekening te houden met het aantal strafbare feiten dat heeft geleid tot een veroordeling door de rechtbank, en niet met het aantal strafbare feiten dat werd vastgesteld door de politiediensten. De basis van het aantal veroordelingen biedt immers meer garanties dat de bewaring van de verkeersgegevens wordt 'geactiveerd' "op basis van objectieve en niet-discriminerende factoren". Om deze redenen kan er geconcludeerd worden dat de statistische moeilijkheden de conformiteit van de Belgische gerichte bewaring met de rechtspraak van het Hof van Justitie in de weg kan zitten.

108. **GEOGRAFISCHE ZONES O.B.V. DREIGING –** De elektronische-communicatiemetagegevens in artikel 126/2, § 2 WEC worden bewaard in de geografische zones die bepaald worden door het OCAD, waar het dreigingsniveau ten minste niveau 3 bedraagt en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones. Hierbij wordt verwezen naar de opdracht van het OCAD om op periodieke basis een gemeenschappelijke strategische evaluatie uit te voeren en op punctuele basis een gemeenschappelijke evaluatie uit te voeren. Er kan redelijkerwijs worden aangenomen dat de geografische zone is afgebakend op basis van een objectieve en niet-discriminerende analyse door het OCAD.

Niettemin dient de volgende opmerking te worden gemaakt. Zoals hiervoor beschreven, stelt het OCAD zowel punctuele als strategische dreigingsanalyses op. De punctuele analyses hebben betrekking op bepaalde evenementen zoals EU-tops, festivals etc. De strategische analyses focussen op een bepaalde tendens in de samenleving, zoals extremisme. De bij wet voorziene analyse per geografische zone zit tussen deze twee dreigingsanalyses in, waardoor het OCAD deze momenteel niet aanlevert. Wat hieruit volgt, is de vraag of wat de wetgever vereist in de praktijk kan omgezet worden. Het OCAD zal naar alle waarschijnlijkheid een nieuwe dreigingsanalyse moeten aanreiken om de uitvoering van de wet mogelijk te maken. Om deze reden kan duitvoering van art. 126/3, §2 lid 1 WEC kan daardoor moeilijkheden ondervinden.

109. **STRATEGISCHE GEOGRAFISCHE ZONES –** In de leden 3 tot en met 5 van artikel 126/3 WEC staan de elektronische-communicatiemetagegevens opgesomd die worden bewaard "in de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit", "in de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking" en "in de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen". Deze gebieden worden vervolgens opgesomd in de overeenkomstige leden. Voor elke categorie van zone bedoeld in de paragrafen 3 tot 5, bepaalt de Koning de omvang van de perimeter van de zone. De meerderheid van de rechtsleer[345] geeft evenwel aan dat het gaat om een zeer uitgebreide lijst van strategische geografische zones. In hun geheel beschouwd, kunnen deze zones leiden tot een ruime retentie, een die *de facto* zou kunnen neerkomen op een algemene bewaarplicht. Er zal in de praktijk bekeken moeten worden of de retentie zich in gebied en gebruikers beperkt tot wat strikt

[345] Van ROY en ROYER, VAN DE HEYNING, BERHÉLÉMY, FLUMIAN en FRANSSEN.

noodzakelijk is. 'Strategische locatie' is een begrip dat heel breed ingevuld kan worden als het ter bestrijding van ernstige criminaliteit of waarborging van de nationale of openbare veiligheid is. Zo worden niet alleen het koninklijk paleis of spoorwegstations begrepen onder 'strategische locatie', maar ook autosnelwegen en de bijbehorende openbare parkeerterreinen. Wanneer we kijken naar de manier waarop de wetgever deze bewaarplicht heeft vormgegeven, kan evenzeer de vraag gesteld worden of het Hof van Justitie in zijn rechtspraak niet te veel ruimte liet voor gerichte bewaring, waardoor deze bewaarplicht in de praktijk feitelijk verandert in een vrijwel algemene en ongedifferentieerde bewaring.

110. **BEPERKTE DUURTIJD –** De duurtijd van de bewaring mag ten slotte niet langer zijn dan strikt noodzakelijk in het licht van het nagestreefde doel. In principe worden de gegevens die onder gerichte bewaring vallen gedurende twaalf maanden bewaard. De gegevens bewaard in de geografische zones van artikel 126/3, § 1 WEC wijken af van deze principiële bewaartermijn van een jaar. In dit verband werd een trapsgewijs systeem ingesteld voor de bewaartermijn voor de gegevens op basis van het statistisch criterium. Dit betekent dat afhankelijk van het aantal vastgestelde misdrijven in de georgrafische zone, de bewaartermijn voor de gegevens zes maanden, negen maandag of twaalf maanden bedraagt. De wetgever lijkt op deze manier tegemoet te komen aan het evenredigheidsbeginsel door om een onderscheid te maken tussen de bewaartermijnen naargelang de noodzaak van bewaring. Toch kunnen er bedenkingen gemaakt worden bij de effectiviteit van deze regeling. Ondanks een reeks uitzonderingen komt de regeling er nog steeds op neer dat er een bewaarperiode is van een jaar. Zo worden communicatiegegevens in gemeentehuizen, op autosnelwegen en in treinstations altijd een jaar lang bijgehouden. Bovendien kan de bewaartermijn niet aangepast worden in functie van de omstandigheden van de bewaring.

111. **CONCLUSIE –** De wetgever lijkt te streven naar een brede bewaring van gegevens voor de bestrijding van ernstige criminaliteit en voor de bescherming van de nationale veiligheid, waarbij het startpunt de criteria zijn die worden aangereikt door het Hof van Justitie. De vraag stelt zich daarbij of deze criteria ook in overeenstemming is met het doeltreffendheidsbeginsel van het recht van de Europese Unie. Gelet op de vage invulling van het begrip ernstige criminaliteit, de statistische moeilijkheden, de grote lijst aan strategische geografische zones en de bezorgdheden over de bewaartermijn, komt het niet als een verrassing dat er ondertussen maar liefst vijf vernietigingsberoepen bij het Grondwettelijk Hof zijn ingesteld.

4.3.4.3. Gerichte bewaring in het kader van een strafonderzoek

112. **ALGEMEEN –** Met betrekking tot de gerichte bewaring in het kader van een strafonderzoek, voert de dataretentiewet van 2022 een maatregel in voor het bevriezen van gegevens in real time ("future freeze") in het kader van een onderzoek. Dit gebeurt op het niveau van justitie in het nieuwe artikel 39*quinquies* Sv. en op het niveau van de inlichtingen- en veiligheidsdiensten in het nieuwe artikel 13/6 van de wet inlichtingendiensten. Voor de volledigheid kan nog toegevoegd worden dat de "quick freeze", waarbij een snelle bewaring gevraagd wordt van reeds bestaande gegevens, al bestaat in de Belgische strafprocedure. Deze is voorzien in artikel 39*ter* Sv. De huidige wet voert dus enkel de "future freeze" in als nieuwe maatregel in het Wetboek van strafvordering. Voor de inlichtingendiensten zijn beide vormen van snelle bewaring nieuw: zowel de "quick freeze" als de "future freeze" worden ingevoerd door de dataretentiewet van 2022. Het Hof van Justitie heeft aan het gericht real-time verzamelen van verkeers- en locatiegegevens die uitsluitend betrekking hebben op een of meerdere personen strenge voorwaarden verbonden. Ten eerste moet het gebruik ervan beperkt zijn tot tot personen ten aanzien van wie een gegrond vermoeden bestaat dat zij op enigerlei wijze betrokken zijn bij terroristische activiteiten. In dit verband schreven DE KEERSMAECKER en VAN DE HEYNING echter dat de beperking van realtime bewaring tot terroristische misdrijven een te enge lezing van het arrest zou zijn. Ten tweede moet er een voorafgaande toetsing door een rechter of een onafhankelijk administratief orgaan mogelijk zijn, waarvan de beslissing bindend is, teneinde te waarborgen dat deze real-time inzameling alleen wordt toegestaan binnen de grenzen van het strikt noodzakelijke. Ten derde moet het besluit waarbij het real-time verzamelen van verkeers- en locatiegegevens wordt toegestaan gebaseerd zijn op objectieve criteria die in de nationale wetgeving zijn vastgesteld. Ten laatste moeten de bevoegde nationale autoriteiten die realtime verkeers- en locatiegegevens verzamelen, de betrokken personen daarvan overeenkomstig de toepasselijke nationale procedures in kennis stellen voor zover en zodra die kennisgeving de taken waarvoor die autoriteiten verantwoordelijk zijn, niet langer in gevaar kan brengen.

113. **ART. 39 QUINQUIES SV. –** Bij het opsporen van de misdaden en de wanbedrijven kan de procureur des Konings, wanneer er ernstige aanwijzingen zijn dat de misdrijven een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben een bevel tot gerichte bewaring uitvaardigen. Dit bevel is gericht aan één of meerdere operatoren van een elektronisch communicatienetwerk aan iedereen die een dienst aanbiedt om via een elektronisch communicatienetwerk te communiceren, om de verkeersgegevens bedoeld in artikel 88bis, § 1, eerste lid Sv. die hij noodzakelijk acht en die door hen worden gegenereerd of verwerkt, te bewaren. Belangrijk om te verduidelijken is dat het gaat om het *bewaren* van de gegevens, niet de *toegang* daartoe. Voor de toegang tot die gegevens zal in principe nog steeds een bevel van de onderzoeksrechter op grond van artikel 88bis Sv. vereist zijn. Wie weigert mee te werken of gegevens vernietigt of wijzigt, is strafbaar met een gevangenisstraf van zes maanden tot een jaar en/of met een geldboete van 26 tot 20.000 euro, te vermeerderen met opdeciemen. In het derde lid van de eerste paragraaf wordt bepaald welke vermeldingen in de beslissing van de procureur des Konings moeten worden opgenomen. Er moet op gewezen worden dat in de beslissing specifiek moet worden aangegeven op welke perso(o)n(en), plaats(en) of

communicatiemiddel(en) de bewaring betrekking heeft. De maatregel heeft niet alleen betrekking op gegevens betreffende de verdachte, maar kan ook gegevens omvatten betreffende het slachtoffer, diens sociale of professionele kring, specifieke plaatsen, zoals de plaatsen waar het strafbare feit is gepleegd en/ of voorbereid, of communicatiemiddelen.

114. **GEGRONDE VERMOEDENS** – De met redenen omklede en schriftelijke beslissing moet onder andere het strafbare feit waarop het bevel betrekking heeft vermelden, alsook de feitelijke omstandigheden van de zaak die de bewaring van de gegevens rechtvaardigen en de precieze aanduiding van één of meerdere van de volgende elementen: de persoon of de personen, de communicatiemiddelen of de plaatsen waarop de bewaring betrekking heeft. Bovendien is er de voorwaarde dat het moet gaan om ernstige aanwijzingen dat de misdrijven een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben. Niettemin valt te betwijfelen of de drempel van één jaar correctionele hoofdgevangenisstraf hier wel hoog genoeg ligt. Het Hof van Justitie benadrukte dat realtime-retentie een bijzonder ingrijpende beperking is van de privacy en bescherming van persoonsgegevens omdat het doen en laten van de persoon volledig in kaart gebracht wordt. Dit doet vermoeden dat realtime-retentie slechts als uitzonderlijke maatregel kan ingezet worden gezien de ingrijpende beperking van de fundamentele rechten, namelijk beperkt tot wanneer het strikt noodzakelijk is om ernstige criminele feiten op te lossen of te voorkomen. Om deze reden lijkt het dat de Belgische wetgever niet voldaan heeft aan de eerste voorwaarde.

115. **VOORAFGAANDE TOETSING –** De machtiging moet worden gecontroleerd door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is. In de wetsbepaling is deze mogelijkheid tot controle niet opgenomen. Het wordt ook niet vermeldt in de memorie van toelichting. Om deze reden kan gesteld worden dat er niet voldaan is aan de voorwaarde.

116. **BESLUIT GEBASEERD OP OBJECTIEVE CRITERIA –** Er werd voorzien in een objectieve drempel, namelijk dat er ernstige aanwijzingen moeten zijn dat de misdrijven een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben. Voor ieder misdrijf wordt er weliswaar in de nationale wetgeving voorzien in een straf. Het valt wel op dat, los van de drempel van de hoofdgevangenisstraf, geen bijkomende objectieve criteria aanwezig zijn die het OM aansturen over te gaan tot het bevel tot bewaring. Niettemin lijkt er aan deze voorwaarde voldaan te zijn.

117. **KENNISGEVING –** De persoon die het voorwerp van deze maatregel uitmaakte, moet hier nadien van in kennis gesteld worden, tenzij dit het doel van de retentie in gevaar zou brengen. Over deze kennisgeving is niks terug te vinden in de wet, noch in de memorie van toelichting.. Hoewel er in de praktijk altijd kan overgeggaan worden tot een kennisgeving hiervan aan de betrokken persoon, lijkt het gelet op het feit dat real-time bewaring een zware inmenging teweegbrengt in de rechten en vrijheden van de burgers, noodzakelijk deze kennisgeving expliciet op te nemen in de wetgeving. Aan deze voorwaarde lijkt bijgevolg niet voldaan te zijn.

118. **CONCLUSIE –** Hieruit kan worden geconcludeerd dat de wetgever soepel is omgegaan met het invullen van de voorwaarden. Ondanks dat het nut van realtime-opvolging van verkeers- maar vooral van locatiegegevens voor het oplossen van zaken die betrekking hebben ernstige criminaliteit niet in twijfel wordt getrokken, gaat deze regeling wel in tegen de ratio van de gerichte bewaring in real time. Namelijk dat het als uitzonderlijke maatregel kan ingezet worden gezien de ingrijpende beperking van de fundamentele rechten.

119. **ART. 13/6 WET INLICHTINGENDIENSTEN –** De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een operator van een elektronisch communicatienetwerk of een verstrekker van een elektronische communicatiedienst om over te gaan tot de bewaring van de verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen waarover hij beschikt op het tijdstip van de vordering ("quick freeze") en de bewaring van de verkeers- en lokalisatiegegevens die hij op basis van de vordering genereert en verwerkt ("future freeze"). De inlichtingen- en veiligheidsdiensten houden een register bij van alle vorderingen tot bewaring. Elke beslissing tot vordering en de motivering ervan worden ter kennis gebracht van het Vast Comité I. Indien het Vast Comité I een onwettigheid vaststelt, maakt het een einde aan de vordering. Eenieder die weigert zijn medewerking te verlenen aan de in de paragrafen 1 en 5 bedoelde vorderingen, wordt gestraft met een geldboete van 26 euro tot 20.000 euro.

120. **QUICK FREEZE –** Het bevel tot versnelde bewaring moet volgens het Hof van Justitie worden uitgevaardigd door de bevoegde autoriteit zoals bepaald in het recht van de lidstaat. Ten tweede moet het bevel onderworpen zijn aan effectieve rechterlijke toetsing. Ten slotte moet het beperkt zijn tot een bepaalde termijn. Aan de eerste voorwaarde is voldaan, aangezien de wetgever de inlichtingen- en veiligheidsdiensten heeft aangesteld als bevoegde autoriteit. Met betrekking tot de tweede voorwaarde kan de vraag gesteld worden of de de maatregel onderworpen aan is effectieve rechterlijke toetsing. Volgens de letter van de tekst wordt enkel voorzien in een *ex post* controle door Vast Comité I. Dit comité is een onafhankelijk controleorgaan dat toezicht uitoefent op alle methoden voor het verzamelen van gegevens door de inlichtingendiensten. Ten slotte met betrekking tot de laatste voorwaarde, stelt de bepaling in kwestie dat de bewaartermijn van de gegevens niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure. Er kan gesteld worden dat aan deze voorwaarde voldaan is.

121. **FUTURE FREEZE –** Voor deze bewaring gelden dezelfde voorwaarden als opgesomd in randnummer 112. Ten eerste moet het gebruik ervan beperkt zijn tot tot personen ten aanzien van wie een gegrond vermoeden bestaat dat zij op enigerlei wijze betrokken zijn bij terroristische activiteiten. Ten tweede moet er een voorafgaande toetsing door een rechter of een onafhankelijk administratief orgaan mogelijk zijn, waarvan de beslissing bindend is, teneinde te waarborgen dat deze real-time inzameling alleen wordt toegestaan binnen de grenzen van het strikt noodzakelijke. Ten derde moet het besluit waarbij het real-time verzamelen van verkeers- en locatiegegevens wordt toegestaan gebaseerd zijn op objectieve criteria die in de nationale wetgeving zijn vastgesteld. Ten laatste moeten de bevoegde nationale autoriteiten die realtime verkeers- en locatiegegevens verzamelen, de betrokken personen daarvan overeenkomstig de

toepasselijke nationale procedures in kennis stellen voor zover en zodra die kennisgeving de taken waarvoor die autoriteiten verantwoordelijk zijn, niet langer in gevaar kan brengen.

Met betrekking tot de eerste voorwaarde bepaalt art. 13/6 §2 van de wet inlichtingendiensten dat de vordering onder andere de personen, groeperingen, geografische gebieden, communicatiemiddelen en/of gebruikswijze waarvan de verkeers- en lokalisatiegegevens moeten bewaard worden moet vermelden. In dit verband kan er nogmaals verwezen worden naar de taken van de inlichtingen- en veiligheidsdiensten, zoals uitgeschreven in randnummer 98. Het kan dus redelijkerwijs aangenomen worden dat het gebruik ervan beperkt zijn tot tot personen ten aanzien van wie een gegrond vermoeden bestaat dat zij op enigerlei wijze betrokken zijn bij bedreigingen gericht tegen de nationale veiligheid. Met betrekking tot de tweede voorwaarde wordt er noch in de wet, noch in de memorie van toelichting melding gemaakt vaan een voorafgaande toetsing door een rechter of een onafhankelijk administratief orgaan mogelijk zijn, waarvan de beslissing bindend is, teneinde te waarborgen dat deze real-time inzameling alleen wordt toegestaan binnen de grenzen van het strikt noodzakelijke. Wel wordt er, zoals aangehaald in het vorig randummer, vorozien in een *ex post* controle door Vast Comité 1. Vervolgens wat betreft de het feit dat de verzameling moet gebaseerd zijn op objectieve criteria die in de nationale wetgeving zijn vastgesteld, kan dezelfde kritiek als in randnummer 116 toegepast worden. Er werd niet specifiek voorzien in objectieve criteria ingeschreven in de wet. Ten slotte wordt er geen mogelijkheid ingeschreven voor de kennisgeving aan de betrokken personen voor zover en zodra die kennisgeving de taken waarvoor die autoriteiten verantwoordelijk zijn niet langer in gevaar kan brengen.

122. **CONCLUSIE –** Op basis van het voorgaande kan geconcludeerd worden dat ook in de wet inlichtingendiensten de voorwaarden onvoldoende vorm hebben gekregen.

4.3.5. Toegang tot de bewaarde gegevens

123. **ALGEMEEN –** De bewaring van gegevens en de toegang ertoe vormen onderscheiden inmengingen in de door de artikelen 7 en 11 van het EU-Handvest gewaarborgde grondrechten. Het algemeen principe voor de toegang tot bewaarde gegevens is vastgelegd in nieuw artikel 127/1 WEC. Het doel van dit artikel is verzekeren dat alleen de autoriteiten die bevoegd zijn voor het aangegeven doel van bewaring toegang kunnen krijgen tot deze gegevens. Om deze autoriteiten in staat te stellen deze gegevens te verkrijgen, moet daarin worden voorzien door een formele wettelijke norm. In dit onderdeel zal ten eerste het algemene principe toegelicht worden. Vervolgens worden de artikelen 46bis Sv. voor de toegang tot identificatiegegevens en art. 88bis Sv. voor de toegang tot elektronische-communicatiemetagegevens besproken in het licht van de Unierechtelijke voorwaarden.

124. **ART. 127/1 WEC –** Met het doel om de toegang tot bewaarde gegevens te reguleren op basis van nieuwe criteria, heeft de dararetentiewet van 2022 het nieuwe artikel 127/1 WEC geïntroduceerd. Dit artikel begint met een beschrijving van het begrip "zware criminaliteit", aangezien dit een impact heeft op welke actoren toegang hebben tot de bewaarde gegevens. Het is opvallend dat de wetgever gekozen heeft voor een expliciete invulling van het begrip "zware criminaliteit", gelet op het feit dat dit niet noodzakelijk werd geacht voor de bepaling met betrekking tot de bewaarplicht van de gegevens. In de memorie van toelichting wordt benadrukt dat het begrip verder aangevuld moet worden en in de toekomst gewijzigd kan worden. Deze opsomming van misdrijven die als ernstig kunnen worden beschouwd, laat de wetgever toe om zelf te bepalen wanneer toegang mogelijk is zonder dat op voorhand in de wet vast te leggen. Hierdoor is het niet altijd duidelijk wanneer toegang tot de gegevens mogelijk is volgens de wetgeving. Onder het begrip "zware criminaliteit" vallen nu onder andere: (I) feiten die een minimale correctionele hoofdgevangenisstraf bedoeld in artikel 88bis, § 1, eerste lid Sv. tot gevolg kunnen hebben, (II) feiten die kunnen leiden tot een sanctie van niveau 5 of 6 zoals bedoeld in artikel XV.70 WER en (III) feiten die een inbreuk zouden vormen op artikel 14 of 15 Verordening Marktmisbruik of bepalingen genomen op basis of ter uitvoering van deze artikelen. 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 WEC. Bij elke operator wordt een Coördinatiecel opgericht, belast met het verstrekken aan de wettelijk bevoegde autoriteiten, op hun verzoek, van de elektronische-communicatiegegevens.

De tweede en derde paragraaf van art. 127/1 WEC koppelen de toegang tot de identificatiegegevens aan bepaalde bevoegde autoriteiten. Meer concreet wordt er een opsomming gemaakt van tien bevoegde autoriteiten die toegang kunnen krijgen tot deze gegevens voor de doelstellingen die de wetgever voorschrijft. Zo mogen bijvoorbeeld 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 (5°) en administratieve of gerechtelijke autoriteiten die criminaliteit in het algemeen bestrijden (8°), toegang nemen tot deze gegevens.

Dit kan enkel voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

In vergelijking met de identificatiegegevens is de toegang tot elektronische communicatiemetagegevens en IP-adressen toegewezen aan de bron beperkter. Een verzoek van een autoriteit om van een operator een IP-adres te krijgen dat is toegewezen aan de bron van een verbinding is 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. Enkel de inlichtingen- en veiligheidsdiensten (1°), de bevoegde autoriteiten die optreden om ernstige bedreigingen voor de openbare veiligheid te voorkomen (2°), de autoriteiten belast met het vrijwaren van de vitale belangen van natuurlijke personen (3°), 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 (6°) en 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 (9°) hebben toegang tot de gegevens bewaard in de artikelen 126/1 en 126/3 WEC (elektronische communicatiegegevens). Dit kan ook weer voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

125. **AANDACHTSPUNTEN –** De verschillende toegangsbevoegdheden en de link met de beoogde doelstellingen door de verschillende actoren zijn in overeenstemming met de jurisprudentie van het Hof van Justitie. De toegang, als afzonderlijke verwerking van gegevens, is enkel mogelijk voor de in artikel 15, eerste lid e-Privacy Richtlijn opgesomde doelstellingen, met name het waarborgen van de nationale veiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem. De wetgever heeft deze doeleinden expliciet opgesomd bij het specifiëren van de actoren die toegang hebben tot de bewaarde gegevens. De dataretentiewet van 2022 is op dit punt voldoende duidelijk. Uit het voorgaande volgt dat toegang tot de bewaarde gegevens mogelijk is voor dezelfde doelstelling die de bewaring kan rechtvaardigen. Ook op dit punt is de dataretentiewet van 2022 in overeenstemming met de voorwaarden van het Hof van Justitie. Voor het uitwerken van de materiële en procedurele voorwaarden koppelt de wetgever terug naar een "formele wettelijke norm". De wetgever zal erop moeten toezien dat enkel de strikt noodzakelijke gegevens op basis van die wettelijke norm kunnen worden opgevraagd en alleen voor de gepaste doeleinden.

126. **TOEGANG IN HET KADER VAN EEN STRAFONDERZOEK –** Opdat de gerechtelijke autoriteiten de voor justitiële doeleinden opgeslagen gegevens kunnen verkrijgen, moet daarin worden voorzien door een formele wettelijke norm. Deze formele wettelijke norm is in dit geval het Wetboek van Strafvordering. De nieuwe dataretentie verandert niet wezenlijk de manier waarop gerechtelijke autoriteiten toegang hebben tot deze gegevens in het kader van

strafrechtelijke onderzoeken. Toch wordt er even stilgestaan bij art. 46*bis* Sv. dat de toegang tot identificatiegegevens regelt, en art. 88*bis* Sv. dat de toegang tot elektronische-communicatiemetagegevens behandelt.

127. **ART. 46*BIS* SV. –** Dit artikel geeft het openbaar ministerie toegang tot identificatiegegevens, opgesomd in artikel 126 WEC. Deze gegevens moeten voortaan worden bewaard voor zover de exploitant ze beheert of verwerkt. Volgens het Hof van Justitie is een dergelijke toegang slechts een beperkte inbreuk op de fundamentele rechten uitmaakt waarbij de proportionaliteit moet beoordeeld worden door de afweging van de ernst van het misdrijf en de inbreuk op de vertrouwelijkheid van elektronische communicatiegegevens alsook de bescherming van persoonsgegevens. De toegang op basis van art. 46*bis* Sv. is gericht op het opsporen van misdaden en wanbedrijven, wat geheel in de lijn licht van de rechtspraak van het Hof van Justitie. De motivering weerspiegelt de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad. Voor strafbare feiten die geen correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, kan de procureur des Konings de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan zijn beslissing. Het Openbaar Ministerie mag ook IP-adressen kunnen blijven opvragen, zij het dat enkel toegestaan wordt 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. Deze bepaling lijkt in conclusie overeen te stemmen met de rechtspraak van het Hof van Justitie.

128. **Art. 88*BIS* SV.** – Met betrekking tot de toegang van bevoegde nationale tot de bewaarde verkeers- en locatiegegevens, heeft het Hof erop gewezen dat alleen de bestrijding van zware criminaliteit een dergelijke toegang tot bewaarde gegevens kan rechtvaardigen. Daarnaast legt het Hof een aantal strikte voorwaarden op. De regeling moet ook voorzien in duidelijke en nauwkeurige materiële en procedurele voorwaarden vaststellen voor de toegang tot de bewaarde gegevens. Daarnaast moet het duidelijke en nauwkeurige regels bevatten die aangeven wanneer en hoe de aanbieders van elektronische communicatiediensten aan de bevoegde nationale autoriteiten toegang tot die gegevens moeten verlenen. Bovendien moet er voorzien zijn in een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit. Ten slotte moet er voorzien zijn in een kennisgeving zodra deze kennisgeving het onderzoek niet langer in gevaar brengt.

Wat betreft het nagestreefde doel, moet opgemerkt worden dat niet elk misdrijf waarop een correctionele hoofdgevangenisstraf van één jaar of meer staat, noodzakelijk overeenstemt met een ernstig misdrijf. Wat betreft de voorwaarde om te voorzien in duidelijke en nauwkeurige materiële en procedurele voorwaarden, moet vermeld worden dat wat de termijnen betreft, de wetgever de eerder door het Grondwettelijk Hof nietig verklaarde termijnen opnieuw heeft opgenomen. Voor terroristische misdrijven mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan het bevelschrift. Voor de in art. 90*ter* genoemde strafbare feiten, gepleegd in het kader van een criminele organisatie

of van dien aard dat zij kunnen leiden tot een correctionele gevangenisstraf van vijf jaar of een zwaarder feit voor een periode van negen maanden. Voor andere strafbare feiten kan de onderzoeksrechter de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift. In dit artikel wordt dus een beperkte termijn werd voorzien voor het opvragen van deze gegevens afhankelijk van de ernst van de misdrijven. In art. 88*bis* Sv., art. 127/1 en 127/3 WEC worden verdere procedurele voorwaarden vastgelegd. Ten slotte wordt er een regeling voorzien ter bescherming van het beroepsgeheim van advocaten en artsen. De maatregel tot het verkrijgen van gegevens kan slechts worden uitgevoerd nadat de voorzitter van de balie of de vertegenwoordiger van de provinciale orde van geneesheren daarvan in kennis is gesteld. De onderzoeksrechter deelt hen mee welke elementen volgens hem onder het beroepsgeheim vallen en deze elementen worden niet in het proces-verbaal opgenomen. Aan deze voorwaarde lijkt bijgevolg voldaan. Ten derde wat betreft de regels die aangeven wanneer en hoe de aanbieders van elektronische communicatiediensten aan de bevoegde nationale autoriteiten toegang tot die gegevens moeten verlenen, moet er opnieuw verwezen worden naar art. 127/3 WEC. Met betrekking tot de voorwaarde van een rechterlijke instantie of een onafhankelijke bestuurlijke entiteit, is hieraan voldaan gelet op het evenwicht dat wordt gevonden tussen de belangen die verband houden met de doeltreffendheid van het strafrechtelijk onderzoek en het recht op gegevensbescherming van de personen die door die toegang worden getroffen. Hoewel het theoretisch gezien mogelijk is dat de onderzoeksrechter zijn onafhankelijkheid als rechterlijke instantie behoudt, is de praktijk dat dezelfde persoon als onafhankelijike instantie optreedt en als betrokkene bij het onderzoek. Ten slotte wat betreft de kennisgeving, is dit niet terug te vinden in de wet, noch in de memorie van toelichting.

129. **CONCLUSIE –** De wetgever lijkt zich bewust van de draagwijdte van de rechtspraak van het Hof van Justitie over de toegang tot de gegevens. Toch lijkt de toegang op basis van art. 88*bis* Sv. op de hierboven aangehaalde punten herbekeken te worden.

5. CONCLUSIE

130. Het opzet van deze masterscriptie is een normatieve en evaluatieve analyse van de nieuwe Belgische dataretentiewet van 2022 in het licht van het Unierechtelijk kader. Het antwoord op de onderzoeksvraag moet duidelijk maken in welke mate de Belgische dataretentiewet van 2022 voldoet aan het Unierechtelijke kader en in welke mate uit deze analyse een noodzaak voortvloeit om dit kader te optimaliseren.

131. Om op deze vraag te antwoorden is het belangrijk om dataretentie te zien in het groter maatschappelijk plaatje. Dateretentie is namelijk in de laatste jaren het speerpunt geworden van het veiligheid-versus-vrijheid-debat. In een snel evoluerende digitale samenleving lijdt het geen twijfel dat dataretentie een nuttig instrument is dat de overheid waardevolle informatie kan verschaffen. Het nut van een dergelijke maatregel mag echter geenszins de noodzaak van het gebruik ervan bepalen. Dataretentie maakt namelijk een inmenging mogelijk in de rechten en vrijheden van burgers, wat vragen doet rijzen rond de doelstelling en proportionaliteit ervan. Tegen deze achtergrond is het essentieel om in het veiligheid-versus-vrijheid-debat beide waarden te erkennen waarvoor ze staan en drogredenen te identificeren om uiteindelijk een evenwicht te kunnen bereiken. Het niets-te-verbergen-argument, het alles-of-niets-argument, de kritische benadering van het veiligheidscriterium en de maatschappelijke waarde van privacy zijn enkele van deze elementen die moeten geïdentificeerd en genuanceerd worden vooraleer er kan bijgedragen worden tot een constructief debat.

132. Er wordt door de Europese en nationale wetgevers en rechtscolleges gezocht naar het juiste evenwicht tussen het belang van het verzamelen van informatie voor strafrechtelijke onderzoeken en veiligheid enerzijds en de impact op het privéleven en andere grondrechten anderzijds. Hiervoor is een belangrijke rol weggelegd voor het Hof van Justitie. Over het algemeen genomen is de rechtspraak van het Hof van Justitie over dataretentie geëvolueerd, waarbij elk arrest zich heeft vertaald in een verdere ontwikkeling van voorwaarden en een verdere verfijning van zijn standpunt. Het Hof van Justitie heeft met andere woorden de kans gekregen om zijn oorspronkelijke uitspraken in de zaak *Digital Rights Ireland* verder uit te werken en een evenwicht te zoeken tussen zowel het handhaven van grenzen aan dataretentie als het handhaven van de bescherming van grondrechten.

133. Het Hof bevestigde in zijn arresten dat een preventieve algemene retentie van verkeers- en locatiegegevens enkel verantwoord is voor de bescherming van de nationale veiligheid. Uit de rechtspraak blijkt ook dat gerichte bewaring van verkeer– en locatiegegevens wel mogelijk is voor de bestrijding van ernstige criminaliteit, bescherming van de openbare veiligheid en bescherming van de nationale veiligheid indien er een voldoende objectieve verantwoording is voor deze bewaring en deze niet-discriminatoir is. De gerichte retentie van verkeers- en locatiegegevens wordt als een proportionele inperking van fundamentele rechten beschouwd indien deze beperkt zijn tot bepaalde categorieën van personen, strategische plaatsen en bepaalde geografische zones. In tegenstelling tot verkeers- en locatiegegevens, oordeelde het Hof van Justitie dat de bewaring van identificatiegegevens een geen ernstige inbreuk vormt op

het privéleven en de bescherming van persoonsgegevens. Met betrekking tot de real-time bewaring van verkeers- en locatiegegevens, is dit ook enkel gerechtvaardigd ter bescherming van de nationale veiligheid, mits er voldaan is aan de opgelegde voorwaarden. Ten slotte wat betreft de versnelde bewaring van verkeers- en locatiegegevens, wordt dit slechts gerechtvaardigd voor de bescherming van ernstige criminaliteit, openbare veiligheid en nationale veiligheid. Het bevel tot versnelde bewaring moet worden uitgevaardigd door de bevoegde autoriteit, moet onderworpen zijn aan effectieve rechterlijke toetsing en beperkt zijn tot een bepaalde termijn. De toegang moet bovendien beperkt tot de doeleinden waarvoor het bevel is uitgevaardigd.

Naast de vraag over welke gegevens bewaard mogen worden onder welke omstandigheden, ging het Hof van Justitie in haar rechtspraak ook in op de toegang tot deze gegevens. De regel over de toegang tot gegevens door autoriteiten kan dan ook samengevat worden als "qui peut le plus, peut le moins". Een autoriteit mag voor een bepaalde doelstelling wel toegang nemen tot gegevens bewaard voor een minder zwaarwichtige doelstellingen, maar niet tot gegevens bewaard voor een zwaarwichtigere doelstelling. Daarnaast boog het Hof zich over de vraag wie toegang kan nemen tot de bewaarde gegevens. Als antwoord op deze vraag, stelt het Hof dat wie toegang mag nemen afhankelijk is van het type van bewaarde gegevens en stelde vervolgens voorwaarden voor de instanties die toegang willen verkrijgen.

134. Uit de analyse van de dataretentiewet van 2022 wordt duidelijk dat de Belgische wetgever de Europese criteria zoveel mogelijk heeft proberen omzetten, maar er niet altijd in is geslaagd om dit op een adequate manier te doen. Zo kan de bepaling over versleuteling aanleiding geven tot juridische procedures vanuit de bescherming van het recht op privacy en persoonsgegevens. Wat betreft de algemene en ongedifferentieerde verzameling van verkeers- en locatiegegevens vastgelegd in art. 126/3, §2 tweede lid WEC, bevat de regeling geen duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel. Daarnaast wordt er door de telecomwet geen effectieve toetsing ingevoerd hetzij door een rechtbank, hetzij door een onafhankelijke administratieve instantie waarvan de beslissing bindend is. De regeling van de gerichte bewaring in de telecomwet is op verschillende punten aan verbetering toe. Zo kan het gebrek aan een duidelijke invulling van het begrip zware criminaliteit aanleiding geven tot misbruik, of op zijn minst tot een bepaalde mate aan rechtsonzekerheid. Het statistisch criterium dat wordt gehanteerd om het aantal strafbare feiten vast te stellen per geografische zone kan de conformiteit met de rechtspraak van het Hof van Justitie in de weg kan zitten. Dit staat los van het feit dat de lijst van strategische geografische zones zeer uitgebreid is en *de facto* kan neerkomen op een algemene bewaarplicht. Ondanks dat er een trapgsewijs systeem wordt ingesteld voor de bewaartermijn voor de gegevens op basis van het statistisch criterium, komt de regeling er nog steeds op neer dat voor de meeste gegevens een bewaarperiode is van een jaar bestaat. Met betrekking tot de gerichte bewaring in het kader van een strafonderzoek, kan geconcludeerd worden dat de wetgever de criteria aangereikt door het Hof soepel heeft ingevuld en dat deze regeling ingaat tegen de ratio van de gerichte bewaring in real time. Ten slotte wat betreft de toegang tot de bewaarde gegevens, moet de invulling van zware criminaliteit en de kennnisgeving terug onder de loep genomen worden.

135. De nieuwe Belgische dataretentiewet van 2022 is niet vrij van kritiek wat betreft de overeenstemming ervan met het Unierechtelijk kader. Het voldoet dus met andere woorden niet volledig aan de gestelde criteria. Deze wet is ongetwijfeld niet het laatste hoofdstuk van de dataretentiesaga, mede gelet op het feit dat er intussen maar liefst vijf vernietigingsberoepen bij het Grondwettelijk Hof zijn ingesteld. Het Belgische dataretentiekader zal in het licht van de aankomende beroepen bij het Grondwettelijk Hof en de verwachte arresten van het Hof van Justitie geoptimaliseerd moeten worden.

136. Wat betreft de optimalisatie van het kader moet er ook naar het Europees niveau verwezen worden. De Belgische dataretentiewet van 2022 illustreert hoe lidstaten binnen de vastgestelde grenzen van het Hof van Justitie een wettelijk kader voor dataretentie proberen mogelijk te maken. Sommige lidstaten stappen af van een algemene bewaring terwijl anderen zich wagen aan het tot stand brengen van een nieuw evenwicht zoals uitgewerkt door het Hof van Justitie. Bij wijze van voorbeeld heeft Oostenrijk geen nieuwe regels omtrent dataretentie aangenomen na de vernietiging van de nationale wetgeving die de dataretentierichtlijn implementeerde in afwachting van verdere duiding door het Hof van Justitie. Gezien deze verschillende reacties en de onbeantwoorde prejudiciële vragen, lijkt het erop dat de dataretentiesaga nog even zal voortduren. Niettemin blijven er vragen open en zullen er in de toekomst alleen maar vragen bijkomen. Wanneer deze onbeantwoord blijven, kunnen deze de inspanningen hinderen van de lidstaten die een evenwichtige regeling voor dataretentie tot stand proberen te brengen. De nationale rechtscolleges blijven voor de moeilijke taak staan om een evenwicht te vinden tussen de bescherming van de privacy en persoonsgegevens enerzijds en van de veiligheid van de natie en openbare orde anderzijds.

137. De rol die het Hof van Justitie hierin speelt bestaat slechts in het vaststellen van de grenzen die noodzakelijk worden geacht om de wetgeving in overeenstemming te brengen met het proportionaliteitsbeginsel en het EU-Handvest. De beperkingen gelden zowel voor de EU-wetgever als, bij gebreke van EU-maatregelen, voor de nationale wetgever. Gelet op het feit dat er een Europese incoherentie bestaat over de juiste benadering van dataretentie en gelet op de onzekere status van dataretentie *an sich*, ontstaat er de nood om dit kader op Unieniveau te optimaliseren. In deze specifieke context lijkt het aangewezen dat de EU-wetgever secundaire wetgeving vaststelt over het bewaren van en de toegang tot gegevens om alle betrokken spelers juridische duidelijkheid te verschaffen. Op deze manier kan er een einde komen aan de impasse waarin de het Hof van Justitie en de lidstaten verkeren sinds de ongeldigverklaring van de dateretentierichtlijn in het *Digital Rights Ireland arrest*. Bovendien is de inwerkingtreding van de e-Privacy Verordening die de e-Privacy Richtlijn zal vervangen, met inbegrip van artikel 15, lid 1, daarvan, nog steeds niet in zicht. Het door de EU-wetgever vastgestelde secundaire recht moet derhalve in overeenstemming zijn met deze jurisprudentie en mag niet proberen deze te omzeilen.

6. BIJLAGEN

Bijlage 1 – Schematisch overzicht van de dataretentiewet van 2022

Hoofdstuk 1: Algemene bepaling			
Artikel van de Dataretentiewet	Onderwerp		
Art. 1	Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.		
Hoofdstuk 2: Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie			
Artikel van de dataretentiewet	Artikel van de telecomwet	Wat?	Onderwerp
Art. 2	Art. 2	Invoeging	Definitie fraude, kwaadwillig gebruik van het netwerk of van de dienst, oproeppoging zonder resultaat, elektronische-communicatiegegevens, inhoud van elektronische communicatie en elektronische-communicatiemetagegevens
Art. 3	Art. 107/5	Vervanging	Versleuteling
Art. 4	Art. 121/8	Invoeging	Maatregelen te nemen door de operator in geval van fraude of kwaadwillig gebruik van het netwerk
Art. 5	Art. 122	Wijziging	Verwerking door een operator van de verkeersgegevens voor zijn eigen behoeften/in het belang van zijn abonnees
Art. 6	Art. 123	Wijziging	Verwerking door een operator van de locatiegegevens buiten verkeersgegevens voor zijn eigen behoeften/ in het belang van zijn abonnees
Art. 7	Art. 125, §2	Opheffing	Vereenvoudig van de Telecomwet
Art. 8	Art. 126	Vervanging	(Technische-) identificatiegegevens te bewaren door een operator voor de autoriteiten op algemene en ongedifferentieerde wijze
Art. 9	Art. 126/1	Invoeging	Doelgerichte bewaring op geografische basis: principes

Art. 10	Art. 126/2	Invoeging	Doelgerichte bewaring op geografische basis: door de operatoren te bewaren gegevens
Art. 11	Art. 126/3	Invoeging	Doelgerichte bewaring op geografische basis: zones voor de gegevensbewaring
Art. 12	Art. 127	Vervanging	Identificatie van de abonnee en van de gewoonlijke gebruiker van de dienst
Art. 13	Art. 127/1	Invoeging	Vestrekking van de bewaarde gegevens aan de autoriteiten
Art. 14	Art. 127/2	Invoeging	Kwaliteit en beveiliging van de bewaarde gegevens
Art. 15	Art. 127/3	Invoeging	Coördinatiecel en samenwerking tussen de operatoren en de autoriteiten
Art. 16	Art. 133, §1, vijfde lid	Vervanging	Informatie van de operatoren aan de abonnees voordat zij worden opgenomen in een telefoongids of telefooninlichtingen
Art. 17	Art. 145	Wijziging	Strafbepalingen
Hoofdstuk 3: Wijzigingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren			
Artikel van de Dataretentiewet	Artikel van de wet betreffende de beveiliging en de bescherming van de kritieke infrastructuren	Wat?	Onderwerp
Art. 18	Art. 8	Aanvulling	Bezorgen van lijst van gemeenten waar kritieke infrastructuren zich bevinden door ADCC
Hoofdstuk 4: Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector (BIPT-statuutwet)			
Artikel van de Dataretentiewet	Artikel BIPT-statuutwet	Wat?	Onderwerp
Art. 19	Art. 2	Aanvulling	Definities van verzoek om identificatiegegevens en van verzoek om metagegevens
Art. 20	Art. 14, §1, 3°, d	Invoeging	Straf wegens niet-naleving van artikel 15 van de statuutwet

Art. 21	Art. 15	Herstelling	Administratieve procedure: verzoek om identificatiegegevens, verzoek om metagegevens en verzoek om toegang te verkrijgen tot een databank
Art. 22	Art. 24	Aanvulling	Aanwijzing van de officieren van gerechtelijke politie belast met de controle van de verzoeken
Art. 23	Art. 25	Wijzigingen	Coherentie van de terminologie
Art. 24	Art. 25/1	Invoeging	Strafprocedure: verzoek om identificatiegegevens, verzoek om metagegevens en verzoek om toegang te krijgen tot een databank
Hoofdstuk 5: Wijzigingen van het Wetboek van strafvordering			
Artikel van de Dataretentiewet	Artikel Sv.	Wat?	Onderwerp
Art. 25	Art. 39*quinquies*	Invoeging	Nieuwe wettelijke basis voor bevel tot gerichte bewaring in het kader van een strafonderzoek
Art. 26	Art. 46*bis*	Wijzigingen	Vordering medewerking van operator van een elektronisch communicatienetwerk en dienst binnen het Belgisch grondgebied die bestaat in het overbrengen van signalen via elektronische communicatienetwerken of in staat stellen via dit netwerk informatie te verkrijgen, ontvangen of verspreiden. Opheffing 2 leden Verstrekking real time gegevens Geheimhoudingsplicht
Art. 27	Art. 88*bis*	Wijziging	Bevelschrift, strafbare feiten en bewaartermijn Regeling beroepsgeheimhouders
Hoofdstuk 6: Wijzigingen van de wet van 5 augustus 1992 op het politieambt			
Artikel van de Dataretentiewet	Artikel wet op het politieambt	Wat?	Onderwerp

Art. 28	Art. 42	Aanvulling	Opvordering gegevens door een officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie en modaliteiten ervan
Hoofdstuk 7: Wijzigingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten			
Artikel van de Dataretentiewet	Artikel wet inlichtingen- en veiligheidsdiensten	Wat?	Onderwerp
Art. 29	Art. 3	Aanvulling	Aanvulling definitie
Art. 30	Art. 7	Invoeging	Aanvulling terminologie opdracht van de Veiligheid van de Staat
Art. 31	Art. 11	Invoeging	Aanvulling terminologie
Art. 32	Afdeling 3/1	Invoeging	Vorderingen tot bewaring
Art. 33	Art. 13/6	Invoeging	Bevriezen van gegevens in real time in het kader van een onderzoek op het niveau van de inlichtingen- en de veiligheidsdiensten (quick and future freeze?)
Art. 34	Art. 13/7	Invoeging	Medewerking vorderen van de operatoren van een elektronisch communicatienetwerk en de verstrekkers van een elektronische communicatiedienst om over te gaan tot de algemene en ongedifferentieerde bewaring van de door hen gegenereerde en verwerkte verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen.
Art. 35	Art. 16/2, §2	Wijzigingen	Vervanging van eerste lid en aanpassen terminologie
Art. 36	Art. 18/7	Wijzigingen	Aanpassing terminologie
Art. 37	Art. 18/8	Vervanging	Toegang tot de gegevens met betrekking tot elektronische communicatie door de inlichtingen- en veiligheidsdiensten
Art. 38	Art. 18/14	Vervanging	Aanpassing terminologie ter bevordering van de leesbaarheid
Art. 39	Art. 18/17	Vervanging	Aanpassing terminologie ter bevordering van de leesbaarheid

Hoofdstuk 8: Wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten			
Artikel van de Dataretentiewet	Artikel van de wet betreffende het toezicht op de financiële sector en de financiële diensten	Wat?	Onderwerp
Art. 40	Art. 81	Wijzigingen	Aanpassing terminologie
Art. 41	Art. 84	Invoeging	Quick freeze
Hoofdstuk 9: Wijzigingen 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 (NIS-wet)			
Artikel van de Dataretentiewet	NIS-wet	Wat?	Onderwerp
Art. 42	Art. 62	Vervanging	Nieuwe formulering van artikel 62 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.
Art. 43	Art. 65, §2	Invoeging	Invoeging van de woorden "elektronische-communicatiegegevens" om te voldoen aan art. 23, lid 2, (b) AVG
Hoofdstuk 10: Wijzigingen van de wet van 24 januari 1977 betreffende de bescherming van de gezondheid van de verbruikers op het stuk van de voedingsmiddelen en andere produkten			
Artikel van de Dataretentiewet	Artikel wet betreffende de bescherming van de gezondheid van de verbruikers op het stuk van de voedingsmiddelen en andere produkten	Wat?	Onderwerp
Art. 44	Art. 11, §1	Vervanging	Dit artikel voert de mogelijkheid in om een identiteit te achterhalen op grond van het IP-adres of telefoonnummer, in navolging van de nieuwe bepalingen

			in artikelen 127, § 1, en 127/1, § 1, van de Telecomwet
Hoofdstuk 11: Overgansgbepalingen			
Art. 45	- De gerichte gegevensbewaring op basis van de criteria bedoeld in artikel 126/3, §§ 3 tot 5, van de Telecomwet treedt in werking op de door de Koning bij een besluit vastgesteld na overleg in de Ministerraad bepaalde datum en uiterlijk op 1 januari 2027. - Bij de eerste toepassing van artikel 126/3, §§ 3 tot 5, van de wet van 13 juni 2005 betreffende de elektronische communicatie, maken de in artikel 126/3, § 6, tweede lid, van dezelfde wet bedoelde bevoegde autoriteiten de nodige informatie over aan de de door de Koning aangewezen dienst op een datum die vastgesteld wordt bij het in het eerste lid bedoelde koninklijk besluit en uiterlijk op 1 januari 2026.		
Art. 46	- De ministers van Justitie en van Binnenlandse Zaken bepalen de bewaartermijn van de gegevens bedoeld in artikel 126/2, § 2, van de Telecomwet, per gerechtelijk arrondissement en per politiezone, en op basis van de criteria bedoeld in artikel 126/3, § 1, van dezelfde wet, die zal gelden vanaf de inwerkingtreding van deze wet tot de publicatie van het ministerieel besluit bedoeld in artikel 126/3, § 1, tiende lid, van dezelfde wet.		
Art. 47	Uiterlijk op de eerste dag die volgt op de afloop van een termijn van twee jaar die ingaat op de dag waarop deze wet wordt bekendgemaakt in het Belgisch Staatsblad, bewaren de operatoren de volgende gegevens: - Het MAC-adres, "Media Access Control address", bedoeld in de artikelen 126, § 1, eerste lid, 16°, derde streepje, en 126/2, § 2, 2°, van de Telecomwet - De gegevens die de identificatie en de lokalisatie van de cellen of andere netwerkaansluitpunten van het mobiele netwerk mogelijk maken, die werden gebruikt tijdens de communicatie, waarvan sprake in artikel 126/2, § 2, eerste lid, 6°, van de Telecomwet - De gegevens bedoeld in artikel 126/2, § 2, 8° en 9°, van de Telecomwet		
Art. 48	- De wijzigingen van artikel 127 van de Telecomwet, vervangen bij artikel 12, zijn enkel van toepassing voor de identificaties door de operatoren van de abonnees die gebeuren na de inwerkingtreding van deze wet. - Artikel 127, § 6, tweede lid, van de Telecomwet wordt van kracht twee jaar na de bekendmaking van deze wet. - Tussen de inwerkingtreding van deze wet en de in het tweede lid vastgestelde datum maken de in artikel 127, § 6, tweede lid, van de Telecomwet bedoelde operatoren het voor de abonnees mogelijk om		

	zich te identificeren aan de hand van de documenten bedoeld in artikel 127, § 6, eerste lid, 1° tot 18°, 20° tot 24°, 26°, 28°, en 31°, van diezelfde wet, in het kader van minstens één identificatiemethode van hun keuze. - De operatoren leggen artikel 127, § 7, van de Telecomwet uiterlijk 24 maanden na de bekendmaking van deze wet ten uitvoer. - Wanneer een operator de indirecte identificatiemethode bedoeld in artikel 127, § 10, eerste lid, 3°, van de Telecomwet ten uitvoer legt, bewaart hij de gegevens die erin worden beoogd uiterlijk 24 maanden na de bekendmaking van deze wet. - De operatoren leggen artikel 127, § 10, eerste lid, 6°, en tweede lid, van de Telecomwet uiterlijk 24 maanden na de bekendmaking van deze wet ten uitvoer. De in deze bepalingen bedoelde rechtspersonen verkrijgen de erkenning uiterlijk 24 maanden na de bekendmaking van deze wet.

Bijlage 2 – Te bewaren gegevens in het licht van artikel 126, §1 lid 1 WE

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.

Bijlage 3 – Te bewaren gegevens in het licht van artikel 126/2, §2 WEC

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.

7. BIBLIOGRAFIE

Wetgeving

- Raad van Europa

Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden van 4 november 1950, *BS* 19 augustus 1988, 5.029.

- Europese Unie

Handvest van de Grondrechten van de Europese Unie van 12 december 2007, *Pb.L.* 26 oktober 2012, afl. 326, 391.

Verord. Europees Parlement en de Raad nr. 2016/679, 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 Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pb.L.* 4 mei 2016, afl. 119, 1.

Voorstel (Comm.) voor een Verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie), 10 januari 2017, COM/2017/010 final - 2017/03 (COD).

Richtl. Europees Parlement en de Raad nr. 2002/58, 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), *Pb.L.* 31 juli 2002, afl. 201, 37.

Richtl. Europees Parlement en de Raad nr. 2006/24, 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, *Pb.L.* 13 april 2006, afl. 105, 54.

- België

    - Wetgevende normen

Gecoördineerde Grondwet, BS 17 februari 1994, 4054.

Wetboek van Strafvordering – Eerste boek van 17 november 1808, BS 27 november 1808, 0.

Strafwetboek van 8 juni 1867, *BS* 9 juni 1867, 3133.

Wet van 21 maart 1991 betreffende de hervorming van sommige overheidsbedrijven, *BS* 27 maart 1991, 6155.

Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, *BS* 24 januari 1995, 1542.

Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, *BS* 18 december 1998, 40312.

Wet van 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001, 02.909.

Wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 juni 2005, 28070.

Wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, *BS* 31 december 2021, 126491.

Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *BS* 18 juli 2016, 44.717.

KB 9 januari 2003 tot uitvoering van de artikelen 46bis, § 2, eerste lid, 88*bis*, § 2, eerste en derde lid, en 90quater, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109*ter*, § 2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *BS* 10 februari 2003.

KB van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 8 oktober 2013, 70828.

- Voorbereidende documenten

Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 2000-2001, nr. 50-0213/011.

Wetsontwerp van 4 november 2004 betreffende de elektronische communicatie, *Parl.St.* Kamer 2004-2005, nr. 51-1425/001.

Wetsontwerp van 27 juni 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van Strafvordering, *Parl.St.* Kamer 2012-13, nr. 53-2921/001.

Wetsontwerp van 11 januari 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van elektronische communicatie, *Parl.St.* Kamer 2015-16, nr. 54-1567/001.

Wetsontwerp van 17 maart 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**,** *Parl. St.* Kamer 2021-22, nr. 55-2572/001.

Adv. RvS 28 juni 2021, nr. 69.381/4.

<u>Rechtspraak</u>

- Europees Hof voor de Rechten van de Mens

EHRM 16 december 1992, nr. 13710/88, Niemietz/Duitsland.

EHRM 25 september 2018, nr. 76639/11, Denisov/Oekraïne.

- Hof van Justitie

Concl. A-G H. SAUGMANDSGAARD ØE, ECLI:EU:C:2018:300, bij HvJ (Grote Kamer) Saugmandsgaard 2 oktober 2018, nr. C-207/16, ECLI:EU:C:2018:788, Ministerio Fiscal.

HvJ 20 mei 2003, nrs. C-465/00, C-138/01 en C-139/01, EU:C:2003:294, Österreichischer Rundfunk e.a.

HvJ 23 november 2010, nr. C-145/09, ECLI:EU:C:2010:708, Baden Württemberg/Panagiotis Tsakouridis.

HvJ (Grote kamer) 8 april 2014, nrs. C-293/12 en C-594/12, ECLI:EU:C:2014:238, Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a. en Kärntner Landesregierung e.a.

HvJ 13 mei 2014, nr. C-131/12, EU:C:2014:317, Google Spanje en Google.

HvJ 6 oktober 2015, nr. C-362/14, EU:C:2015:650, Schrems.

HvJ (Grote kamer) 21 december 2016, nrs. C-203/15 en C-698/15, ECLI:EU:C:2016:970, Tele2 Sverige AB/Post-och telestyrelsen en Secretary of State for the Home Department/Tom Watson e.a.

HvJ (Grote kamer) 2 oktober 2018, nr. C-207/16, ECLI:EU:C:2018:788, Ministerio Fiscal.

HvJ (Grote kamer) 6 oktober 2020, nrs. C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, La Quadrature du Net e.a./Premier ministre e.a., French Data Network e.a. en Ordre des barreaux francophones et germanophone e.a./Conseils des ministres.

HvJ (Grote kamer) 6 oktober 2020, nr. C-623/17, ECLI:EU:C:2020:790, Privacy International/Secretary of State for Foreign and Commonwealth Affairs e.a.

HvJ (Grote kamer) 2 maart 2021, nr. C-746/18, ECLI:EU:C:2021:152, H.K. Prokatuur

HvJ (Grote kamer) 5 april 2022, nr. C-140/20, ECLI:EU:C:2022:258, Commissioner of An Garda Síochána.

HvJ (Grote kamer) 20 september 2022, nr. C-793/19 en C-794/19, ECLI:EU:C:2022:702, SpaceNet en Telekom Deutschland.

HvJ (Grote Kamer) 20 september 2022, nr. C-339/20, ECLI:EU:C:2022:703, VD.

Rechtsleer

- Handboeken

BOURDILLON, S. S., PHILIPS, J. en RYAN, M.D., *Privacy vs. Security,* Londen, Springer, 2014, 115 p.

SOLOVE, D., *Nothing to hide: the false tradeoff between privacy and security,* New Haven en Londen, Yale University Press, 2011, vii + 246 p.

WESTIN, A., *Privacy and Freedom*, New York, Atheneum, 1967, xvi + 487 p.

- Tijdschriften

AERTGEERTS, P., "Bewaring van persoonsgegevens en de strijd tegen criminaliteit: een nieuw hoofdstuk" (noot onder HvJ 2 maart 2021, nr. C-764/18, ECLI:EU:C:2021:152, Prokuratuur), *TBP* 2022, 537-539.

BERGHOLM, J., "The Data Retention Safga Continued - from *Tele2 Sverige* to *Privacy International* and *La Quadrature du Net"*, *JFT* 2021, 111-139.

BIJNENS, D., "De wetgeving inzake dataretentie: *the saga continues…*" (noot onder HvJ 21 december 2018, gevoegde zaken nrs. C-203/15 en C-698/15, ECLI:EU:C:2016:970, *Tele2 Sverige AB* en *Secretary of State for the Home Department*), *TBP* 2017, 525-527.

BLAY-GRABARCZYK, L., "Vie privée et nouvelles technologies", *RDLF* 2011, 1.

BRATMAN, B., "Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy, *Tennessee Law Review* 2002, 623-652.

CAIOLA, A., "À la recherche de la justice pondération entre ingérence dans la vie privée et nécessité de lutte contra la criminalité, *RAE* 2018, 719-728.

CAMERON, I., "Balancing data protection and law enforcement needs: Tele2 Sverige and Watson", *CML Rev.* 2017, 1467-1495.

CAMERON, I., "Metadata retention and national security: *Privacy International and La Quadrature du Net*", *CML REV.* 2021, 1443-1471.

CAREEL, S. en ROYER, S., "Voorontwerp dataretentiewet: derde keer, goede keer?", *DJK* 2021, 10-11.

CAVOUKIAN, A., "Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head", *Health and technology* 2017, 329-333.

CELESTE, E., " The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios", *European Constitutional Law Review* 2019, 134–157.

CONINGS, C. en ROYER, S., "Ook hervormde dataretentiewet staat onder druk", *Juristenkrant* 2017, 1.

CONINGS, C., "Dataretentieplicht en privacy" (noot onder GwH 11 juni 2015), *NJW* 2015, 911-913.

DE TERWAGNE, C., "L'illégalité nuancée de la surveillance numérique: la réponse des juridictions belge et française à l'arrêt *La Quadrature du Net* de la Cour de justice de L'Union européenne, RevTrimDrH 2022, 3-27.

DE VILLANFAGNE, F. en DUSOLLIER, S., "La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique", *AM* 2001, 60-81.

DOCKSEY, C., "Ministerio Fiscal: Holding the line on ePrivacy", *Maastricht Journal of European and Comparative Law* 2019, 585-594.

ESKENS, S., "The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature du Net and Others and Privacy International", EDPL 2022, 143-155.

FLAHERTY, D.H., "On the Utility of Constitutional Rights to Privacy and Data Protection, *Case Western Reserve Law Review* 1991, 831-855.

FORGET, C., "L'obligation de conservation des "métadonnées": la fin d'une longue saga juridique?", *Journal des Tribunaux* 2017, 233-239.

FRIED, C., "Privacy.", *The Yale Law Journal* 1968, 475-493.

GELLERT, R. en GURTWIRTH, S., "The Legal construction of privacy and data protection", *Computer Law and Security Review* 2013, 522-530.

KEUNEN, L., "De vernietiting van de Dataretentiewet 2.0: naar een gerichte bewaring met ruimere toegang?" (noot onder GwH 22 april 2021, nr. 57/2021), *RWE* 2021-22, 1464-1471.

KONVITZ, M.R., "Privacy and the law: a Philosophical Prelude.", *Law and Contemporary Problems*, 272-280.

MEESE, J., "Dataretentie: het Hof van Justitie waakt over onze privacy", *RWE* 2016-17, 1639-1640.
NIEUWENHUIS, A., "Review of Privacy vs. Security", *Utrecht Journal of International and European Law* 2015, 137-140.

NISSENBAUM, H., "Protecting Privacy in an Information Age: the Problem of Privacy in Public.", *Law and Philosophy* 1998, 559-596.

PANZAVOLTA, M., ROYER, S. en SEVERIJNS, H., "Algemene dataretentie: ten minste houdbaar tot…?", *T. Strafr.* 2018, 3-18.

REVOLIDIS, I., "H.K. v Prokuratuur: On Balancing Crime INvestigation and Data Protection", *EDPL* 2020, 319-324.

SMUHA, N.A. (noot onder HvJ (grote kamer) 6 oktober 2020, C-623/17 (Privacy International) en gevoegde zaken C-511/18, C-512/18 en C-520/18 (La Quadrature du Net e.a.), *TBP* 2022, 540-543.
SPENCER, S., "Security vs. Privacy", Denver University Law Review 2002, 519-521.

TRACOL, X., "The Joined cases of Dwyer, SpaceNet and VD and SR before the European Court of Justice: The Judgements of the Grand Chamber about data retention continue falling on deaf ears in Member States", *COMPUTER LAW&SECURITY REVIEW* 2023, 1-14.

TRACOL, X., "The two judgements of the European Court of Justice in the court cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is trying hard to square the circle of data retention, *COMPUTER LAW&SECURITY REVIEW 2021,* 1-13.

VAN CANNEYT, T., BERTRAND, A., CROUZET, S. en VANDERDONCKT, L., "Data Protection: CJEU case law review 1995-2020, *Computerrecht* 2021, 78-144.

VAN DE HEYNING, C., "Het moeilijke evenwicht tussen privacy & veiligheid: De impact van het debat over bewaren van communicatiegegevens", *Radices* 2022, 132-161.

VAN DE HEYNING, C., "Overzicht van rechtspraak – Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog", *T.Strafr.* 2019, nr. 1, 38-47.

VAN ROY, L. en ROYER, S., "De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep", *NC* 2023, 1- 22.

WARREN, S.D. en BRANDEIS, L.D., "The right to Privacy, *Harvard Law Review* 1980, 193-220.

- Bijdragen in verzamelwerken

GRABOWSKA-MOROZ, B., "Data retention in the European Union", ZUBIK, M., PODKOWIK, P. en RYBSKI, R. (eds.), *European Constitutional Courts towards Data Retention Laws,* Zwitserland, Springer, 2021, 3 – 19.

LUKACS, A., "What is Privacy? The History and Definition of Privacy." in Keresztes, G. (ed), *Spring Wind 2016,* Budapest, Magyarország:Doktoranduszok Országos Szövetsége, 2016, 256-265.

REGAN, P.M., "Privacy and the common good: revisited", in ROESSLER, B. en MOKROSINKA, D. (eds.), *Social Dimensions of Privacy, Interdisciplinary Perspectives,* Cambridge University Press, 2015, 50-70.

STEEVES, V., "Reclaiming the Social Value of Privacy", in KERR I., STEEVES, V. en LUCOCK, C. (eds.), *Lessons from the Identity Trail: Anonimity, Privacy and Identity in a Networked Society,* New York, Oxford University Press, 191-208.

VEDASCHI, A., "Privacy versus Security: Regulating Data Collection and Retention in Europe. " in GOOLD, B. J. en LAZARUS, L. (eds.), *Security and Human Rights,* Londen, Hart Publishing, 2019, 275-296.

WAGNER DECEW, J., "The feminist critique of privacy: past arguments and new social understandings", in ROESSLER B. en MOKROSINKA D. (eds.), *Social Dimensions of Privacy, Interdisciplinary Perspectives,* Cambridge University Press, 2015, 85-103.

ZUBIK, M., PODKOWIK, J. en RYBSKI, R. (eds.), *Judicial Dialogue on Data Retention in the Digital Age: Concluding remarks,* Cham, Springer, 2021, v + 251 p.

- Overige bronnen

    - Adviezen

EDPS, "Advies 5/2019 over de wisselwerking tussen de e- privacyrichtlijn en de algemene verordening gegevensbescherming, met name wat betreft de taken en bevoegdheden van gegevensbeschermingsautoriteiten", 12 maart 2019, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_nl

BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), *Adviesaanvraag inzake het voorontwerp van wet betreffende de bewaring van gegevens in de elektronische communicatiesector (CO-A-2015-040)*, 9 september 2015, nr. 33/2015, https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-33-2015.pdf.

BESCHERMING VAN DE PERSOONLIJKE LEVENSFEER (CPBL), Adviesaanvraag 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 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 (CO-A-2021-099), 28 juni 2021, nr. 108/2021, https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-108-2021.pdf.

    - Rapporten

KOOMEN, N., "The Encryption Debate in the European Union: 2021 Update, *Carnegie Endowment for International Peace* 2021, 14 p.

- Open brieven

GLOBAL ENCRYPTION COALITION, "Open Letter: 107 organizations and cybersecurity experts call on the Belgian Government to halt legislation to undermine end-to-end encryption, 28 september 2021, www.globalencryption.org/2021/09/open-letter-48-organizations-and-cybersecurity-experts-call-on-the-belgian-government-to-halt-legislation-to-undermine-end-to-end-encryption/.

- Gidsen

EUROPEES HOF VOOR DE RECHTEN VAN DE MENS en RAAD VAN EUROPA, Guide on Article 8 of the European Convention on Human Rights, 2022, www.echr.coe.int/documents/guide_art_8_eng.pdf.

- *Online bronnen*

VSSE, Nationale veiligheidsstrategie, www.premier.be/sites/default/files/articles/NVS_Online_NL.pdf

VAN HORENBEEK, J., "'Met de wortel uitroeien': hoe de politiek de Antwerpse drugsbendes wil aanpakken", *De Morgen* 2023, www.demorgen.be/nieuws/met-de-wortel-uitroeien-hoe-de-politiek-de-antwerpse-drugsbendes-wil-aanpakken~b7dbac79/.

VANHECKE, N., "Hacking treft Antwerpse stadsdiensten in hun kern", *De Standaard* 2022, www.standaard.be/cnt/dmf20221208_97860109.

EUROPEES PARLEMENT, "Proposal for a regulation on privacy and electronic communications", 20 april 2023, www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform.

VAN TOOR, D., "SpaceNet en VD (HvJ EU, C-793/19 en C-339/20) – Here we go again: Duitse en Franse dataretentieregeling(en) in strijd met Unierecht", *European Human Rights Cases Updates* 2023, www.ehrc-updates.nl/commentaar/212435?skip_boomportal_auth=1.