J.J. Oerlemans, M. Hagens & S. Royer[1]

Tijd voor een nieuwe bewaarplicht?

Computerrecht 2021/59

In Nederland en België is er al jarenlang discussie of een bewaarplicht van telecommunicatiegegevens bij aanbieders van elektronische communicatiediensten is toegestaan. In het arrest La Quadrature du Net e.a. biedt het EU Hof van Justitie beperkte mogelijkheden voor het invoeren van een bewaarplicht door lidstaten. Dit artikel analyseert het arrest en maakt duidelijk in welke vorm een bewaarplicht eventueel mogelijk is ter bestrijding van ernstige criminaliteit.

1. Inleiding

Op 6 oktober 2020 heeft het Hof van Justitie van de Europese Unie (hierna: HvJ EU) twee belangrijke arresten[2] gewezen over een bewaarplicht van communicatiegegevens (verkeers-, locatie- en gebruikersgegevens) door EU-lidstaten bij aanbieders van elektronische communicatiediensten.

In dit artikel bespreken we wat de gevolgen zijn van de arresten La Quadrature du Net e.a. en Privacy International ten aanzien van een nationale regeling voor een bewaarplicht in Nederland en België ter bestrijding van ernstige criminaliteit. Het artikel geeft een overzicht van de ontwikkelingen van de regeling tot de bewaarplicht en de jurisprudentie tot dusver. Het biedt bovendien handvatten voor wetgevers onder welke voorwaarden een bewaarplicht mogelijk is die in overeenstemming is met het Handvest van de grondrechten van de Europese Unie (hierna: het Handvest).

Paragraaf 2 bespreekt de achtergrond van de Europese regeling van de bewaarplicht en het nut en de noodzaak ervan. Paragraaf 3 bespreekt kort een overzicht van de jurisprudentie van het HvJ EU omtrent de bewaarplicht en in paragraaf 4 wordt dieper ingegaan op wat het arrest La Quadrature du Net e.a. hierover zegt. Paragraaf 5 bespreekt de gevolgen van deze jurisprudentie voor het wetsvoorstel voor een bewaarplicht in Nederland en paragraaf 6 gaat de gevolgen na voor België.

2. De noodzaak van een bewaarplicht van communicatiegegevens

De noodzaak van een regeling voor een bewaarplicht van gegevens van aanbieders van telecommunicatiediensten werd voor veel EU-lidstaten duidelijk na de aanslagen in Madrid in 2004 en in Londen in 2005. Het idee was dat een Europese richtlijn voor een bewaarplicht de mogelijkheden van effectieve rechtshandhaving – dus ook het voorkomen en vervolgen van terroristisch aanslagen – zou vergroten.[3]

In de kern wordt met een bewaarplicht verzekerd dat gegevens beschikbaar zijn op het moment dat de gegevens nodig zijn voor de uitvoering van belangrijke overheidstaken. De beschikbare gegevens van gebruikers van elektronische communicatiediensten kunnen bijvoorbeeld in een opsporingsonderzoek worden opgevraagd.[4] Het bewaren van gebruikersgegevens en verkeersgegevens vergroot de mogelijkheden personen te identificeren, te lokaliseren en aan te tonen dat personen met anderen in contact hebben gestaan (zie uitgebreid paragraaf 2.1 en 2.2 hieronder).

Het voorstel van de Europese Commissie leidde uiteindelijk tot de Richtlijn 2006/24/EG (de 'dataretentierichtlijn').[5] De richtlijn verplichtte aanbieders van openbare telecommunicatiediensten en -netwerken gebruikersgegevens en verkeersgegevens voor een maximale periode van twee jaar op te slaan ter bestrijding van ernstige criminaliteit.[6] De dataretentierichtlijn vormde een uitzondering op de verplichting in artikel 5 en artikel 6 van de e-Privacyrichtlijn voor aanbieders van openbare elektronische communicatiediensten en -netwerken verkeersgegevens om de vertrouwelijkheid van communicatie te garanderen en gegevens te wissen of anoniem te maken als ze niet langer

1 Prof. mr. dr. Jan-Jaap Oerlemans is bijzonder hoogleraar Inlichtingen en Recht aan de Universiteit Utrecht en senior onderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Dr. Mireille Hagens is senior onderzoeker bij de CTIVD. Dit artikel is op persoonlijke titel geschreven. Dr. Sofie Royer is postdoctoraal onderzoeker bij het Centrum voor IT & IE Recht (CiTiP) en geassocieerd lid van het Instituut voor Strafrecht, beiden KU Leuven.

2 De gevoegde zaken HvJ EU 6 oktober 2020, 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.* (hierna: *La Quadrature du Net e.a.*)) gepubliceerd hierna onder *Computerrecht* 2021/62 en HvJ EU 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790 (*Privacy International/Secretary of State e.a.* (hierna: *Privacy International*)).

3 H. Hijmans, 'De ongeldigverklaring van de Dataretentierichtlijn: een nieuwe stap in de bescherming van de grondrechten door het Hof van Justitie', *NtER* 2014, nr. 7, p. 245-253 (hierna: Hijmans 2014), R. Schoefs, 'Richtlijn gegevensbewaring is dood en begraven', *Juristenkrant* 23 april 2014, 3. Zie over de totstandkoming ook, o.a. L.P. Mol Lous, 'Een Europese bewaarplicht voor verkeersgegevens. De Commissie als bewaker van het opsporingsbelang', *SEW* 2006, 89.

4 In Nederland op grond van artikel 126n e.v. Wetboek van Strafvordering (Sv). In België op grond van de artikelen 46*bis* en 88*bis* Belgisch Wetboek van Strafvordering.

5 Richtlijn 2006/24/EG van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, *PbEU* 2006, L 105/54.

6 Zie artikel 6 Richtlijn 2006/24/EG.

nodig zijn voor het vaststellen van de rekening en bedrijfsvoering.[7]

Tegelijkertijd is de dataretentierichtlijn vanaf begin af aan omstreden geweest.[8] Zoals bekend hebben rechtszaken over de bewaarplicht in veel landen, zoals Nederland, tot de ongeldigverklaring van de nationale implementatie van de door het HvJ EU in Digital Rights (2004) ongeldig verklaarde richtlijn geleid (zie verder paragraaf 3.1 en paragraaf 5). In La Quadrature du Net e.a. laat het HvJ EU dit keer ruimte voor een beperkte vorm van de bewaarplicht (paragraaf 4). Om te bepalen of iets te zeggen valt voor een (hernieuwde) beperkte bewaarplicht van telecommunicatiegegevens ter bestrijding van ernstige criminaliteit, doen wij in deze paragraaf nader onderzoek naar de noodzaak tot het bewaren van gebruikers- en verkeersgegevens.

2.1 *Gebruikersgegevens*

Gebruikersgegevens omvatten kort gezegd de zogenoemde abonneegegevens van de aanbieders van elektronische communicatiediensten.[9] Dat zijn gegevens als de naam en adresgegevens en identificerende gegevens over de apparatuur van de gebruiker van degene die bijvoorbeeld voor een telefoonabonnement betaalt.[10] Als in een opsporingsonderzoek een bepaald telefoonnummer bekend wordt, dan kan een opsporingsambtenaar dus opvragen wie betaalt voor het telefoonabonnement en waar deze persoon woonachtig is. Daarmee kan mogelijk de naam en het woonadres van een verdachte worden achterhaald of een verificatieslag van de identiteit van de verdachte worden uitgevoerd. Het *nut* van het opvragen van gebruikersgegevens in allerlei typen opsporingsonderzoeken is daarmee duidelijk.[11]

De *noodzaak* van een bewaarplicht van deze gegevens voor bestrijding van criminaliteit wordt duidelijk in bepaalde situaties en met name in zaken omtrent cybercriminaliteit. Denk bijvoorbeeld aan de situatie waarbij een middelbare scholier zijn medeleerlingen bedreigt met een 'high school shooting', door een bericht te plaatsen op een internetforum.[12] Bij de forumbeheerder kan in dat geval het IP-adres gevorderd worden, omdat dat doorgaans wordt vastgelegd in de logging van de website (alsmede het tijdstip waarop het bericht is geplaatst). Als in het bericht geen aanwijzingen over de identiteit van de verdachte zijn te vinden, dan kan dat vastgelegde IP-adres het enige beschikbare digitale spoor zijn.[13] Door op te zoeken door welke internet access provider het IP-adres is uitgegeven en de naam- en adresgegevens op te vragen van de abonneehouder kan mogelijk een adres van de verdachte worden achterhaald.[14] Dat kan een cruciale schakel vormen in de opsporing en bewijsvoering voor het delict bedreiging.

In situaties waarbij het aantal beschikbare IPv4-adressen, het IP-adres dat door de provider wordt toegewezen bij toegang tot het internet, veel kleiner is dan het aantal apparaten dat gelijktijdig online is, is het nodig IPv4-adressen gelijktijdig te delen tussen gebruikers. Dit is mogelijk door toepassing van 'carrier grade network address translation'. Deze technieken worden met name toegepast op mobiele netwerken.[15] Aanbieders van mobiele netwerken die van deze technieken gebruikmaken, zijn niet altijd in staat gebruikers van mobiele apparaten te koppelen aan het uitgeven IP-adres. In dat geval levert een vordering van gebruikersgegevens niets op.

De Nederlandse overheid heeft in het rapport 'Mogelijkheden voor identificatie op internet op basis van IP-adres' deze problematiek verder laten onderzoeken. Daaruit blijkt dat in het algemeen de identificatie van abonneehouders op basis van IP-adres en datum/tijd op Nederlandse vaste netwerken goed mogelijk is en met name bij mobiele communicatie dit niet altijd mogelijk is. Het rapport biedt verschillende beleidsopties voor het vergroten van de mogelijkheden gebruikers te identificeren op basis van hun IP-adres met name door nieuwe verplichtingen op te leggen aan aanbieders van telecommunicatiediensten en -netwerken.[16] Dat neemt niet weg dat deze mogelijkheden er niet altijd zijn bij buitenlandse internetproviders en de handhaving van Nederlandse wetgeving

7 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, *PbEU* 2002, L 201/37.

8 Zie over de Richtlijn 2006/24/EG en de Nederlandse implementatie in de Wet bewaarplicht telecommunicatiegegevens: A. Patijn, 'Verplicht opslag van verkeersgegevens?', *Computerrecht* 2003, nr. 2, p. 134-140, A.H.J. Schmidt & G-J. Zwenne, 'Recht en risico. Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatie-verkeersgegevens', *Mediaforum* 2005-9, p. 292-302, M.M. Groothuis, 'De bewaarplicht van verkeersgegevens bij internet en telefonie en de verhouding tot het recht op persoonlijke levenssfeer', *NTM/NJCM-Bulletin* 2006, nr. 6, p. 792-811, H. Franken, 'Wie wat bewaart heeft wat', *RM Themis* 2007/4, p. 125-126, G.-J. Zwenne & A. Schmidt, 'Opmerkingen bij het wetsvoorstel Wet bewaarplicht telecommunicatiegegevens', *Mediaforum* 2008, nr. 7, p. 278-285, G-J. Zwenne & F. Simons, 'Duitse bewaarplicht ongrondwettig. En in Nederland?', *Tijdschrift voor Internetrecht* 2010, nr. 3, p. 87-94.

9 Zie artikel 5 Richtlijn 2006/24/EG.

10 Zie ook de bijlage A en B bij artikel 13.2a van de Telecommunicatiewet.

11 Zie uitgebreid: Odinot e.a., 'De Wet bewaarplicht telecommunicatiegegevens. Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing', WODC, Den Haag: Boom Lemma Uitgevers 2013, p. 82-83 (hierna: Odinot e.a. 2013). Zie ook N. Ferdinandusse, D. Laheij & J.C. Hendriks, 'De bewaarplicht telecomgegevens en de opsporing. Het belang van historische verkeersgegevens voor de opsporing', Openbaar Ministerie & Nationale Politie 2015, p. 3 (hierna: Ferdinandusse, Laheij & Hendriks 2015) en W.N. Ferdinandusse, 'Charlie Hebdo toont belang bewaarplicht telecomgegevens', *NRC Handelsblad* 15 januari 2015.

12 Zie bijvoorbeeld Hof Den Haag 9 maart 2011, ECLI:NL:GHSGR:2011:BP7080.

13 Ferdinandusse, Laheij & Hendriks 2015, p. 3.

14 Zie hierover J.J. Oerlemans, 'Cybercriminaliteit en opsporing', p. 200-206, in: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (red.), *Basisboek Cybercriminaliteit*, Den Haag: Boom criminologie 2020.

15 Zie T. van der Vorst, e.a., 'Mogelijkheden voor identificatie op internet op basis van IP-adres', Dialogic in opdracht van het WODC (Ministerie van Justitie en Veiligheid), Den Haag: nov. 2019, p. 9 (hierna: Van der Vorst e.a. 2019). Ook zijn er niet altijd gebruikersgegevens beschikbaar bij aanbieders van zogeheten 'hotspots', waar een WiFi-verbinding wordt aangeboden. Dat komt onder andere, omdat deze niet altijd een openbare telecommunicatiedienst of -netwerk aanbieden (Odinot 2013, p. 101).

16 Van der Vorst e.a. 2019, p. 10-11.

slechts tot de Nederlandse grenzen reikt, terwijl opsporingsonderzoeken met name naar cybercriminaliteit juist over de territoriale staatsgrenzen reiken. De noodzaak van gebruikersgegevens en het bewaren ervan ten behoeve van criminaliteitsbestrijding is daarmee duidelijk aan te tonen. Deze noodzaak is lastiger vast te stellen bij verkeersgegevens.

2.2 *Verkeersgegevens*

Verkeersgegevens zijn gegevens over de communicatie, zoals wie naar wie belt, waar vandaan, hoe vaak en voor hoelang communicatie plaatsvindt.[17] Ook locatiegegevens die de antenne aangeven waarmee het apparaat verbinding maakt voor communicatie, zijn verkeersgegevens. Het gaat dus uitdrukkelijk niet om de inhoud van communicatie, zoals de inhoud van verstuurde (inmiddels bijna ouderwetse) smsjes, e-mailberichten en zoektermen die zijn ingetypt in een zoekmachine.[18]

Het is hierbij ook belangrijk om te weten dat de bewaarplicht in Nederland gold voor de diensten die zijn aangewezen in de Telecommunicatiewet. Deze bewaarplicht gold niet voor 'Over The Top' (OTT)-diensten, zoals Skype en WhatsApp. Zij verlenen een dienst over het internet, maar niet de internetverbinding zelf.[19] Hierbij is het van belang te signaleren dat de nieuwe 'Telecomcode' (de implementatie van Richtlijn 2018/1972 van 11 december 2018) de Telecommunicatiewet wijzigt. Het toepassingsbereik van de telecomwetgeving met betrekking tot het begrip 'aanbieder van een elektronische communicatiedienst' zal dan worden verruimd tot zogenoemde 'interpersoonlijke communicatiediensten', waar ook OTT-diensten zoals Whatsapp en Gmail onder vallen. Een nieuwe bewaarplicht voor communicatiegegevens die van toepassing wordt verklaard op aanbieders van communicatiediensten, kan in de toekomst mogelijk ook voor OTT-diensten gelden. Het handhaven van dergelijke nationale wetgeving op bedrijven met hun hoofdkwartier in het buitenland zal echter niet eenvoudig zijn en nieuwe internationale afspraken vereisen.[20]

Verkeersgegevens blijken in ieder geval *nuttig* voor opsporingsonderzoeken. De gegevens worden ook vaak in het kader van een opsporingsonderzoek[21] gevorderd. In Nederland zijn hier slechts één keer statistieken over verstrekt. In het jaar 2012 betroffen het in totaal 41.658 vorderingen. De vorderingen bij aanbieders van communicatiediensten (voornamelijk telecombedrijven die (mobiele) telefoon en internetabonnement aanbieden) hadden betrekking op de categorie 'historische verkeersgegevens telecommunicatie' (verkeersgegevens).[22] Uit het evaluatieonderzoek 'De Wet bewaarplicht telecommunicatiegegevens' van Odinot e.a. (2013) blijkt dat deze gegevens in de praktijk met name worden gebruikt ter lokalisering van personen (waar is een apparaat in gebruik bij een persoon op welk moment?) en als bewijs voor het feit dat een persoon met anderen in contact heeft gestaan.[23] Het kan daarbij gaan over verdachten, maar de gegevens kunnen bijvoorbeeld worden gebruikt om de verklaring van een getuige te controleren dat hij op een bepaald moment met anderen in contact heeft gestaan.[24]

Voor de bepaling van de locatie van een mobiele telefoon van een bepaalde gebruiker wordt de locatie van een zendmast gebruikt op de plek waar de communicatie wordt gestart ('First Cell ID'). Deze zendmasten hebben een bepaald bereik waardoor opsporingsdiensten bij benadering kunnen zien waar de desbetreffende telefoon is geweest bij aanvang van het gesprek. Plaatsbepaling door middel van historische verkeersgegevens kan antwoord geven op vragen zoals: waar woont iemand, was iemand in de buurt van de plaats delict, wat waren de reisbewegingen van iemand en op welke locatie heeft iemand het laatste gebeld.[25] De auteurs van het evaluatierapport komen tot de conclusie dat verkeersgegevens een 'belangrijke en zeer gewaardeerde rol spelen in de opsporingspraktijk'.[26] Dit beeld wordt bevestigd in een rapport van de Nationale Politie en het Openbaar Ministerie uit 2015, waarin 130 zaken worden uitgelegd waarbij verkeersgegevens een belangrijke rol hebben gespeeld in de opsporing en vervolging van misdrijven.[27]

Toch is het beeld dat naar voren komt uit de rapporten dat verkeersgegevens weliswaar nuttig en waardevol zijn voor opsporingsonderzoeken, maar dat de *noodzaak* niet voldoende duidelijk wordt. Volgens Ferdinandusse e.a. (2015) is de reden dat de noodzaak niet kan worden aangetoond omdat opsporingsmethoden altijd in onderlinge samenhang worden gebruikt, waardoor de zelfstandige bijdrage

17 Zie voor een meer specifieke opsomming bijlage A en B bij artikel 13.2a van de Telecommunicatiewet.

18 Odinot 2013, p. 97. In de praktijk blijkt het soms lastig een onderscheid te maken tussen de inhoud van communicatie en verkeersgegevens. Zie ook p. 60 van het rapport van de evaluatiecommissie Jones-Bos op de Wet op de inlichtingen- en veiligheidsdiensten 2017 (*Kamerstukken II* 2020/21, 34588, nr. 88 (bijlage). De categorieën van gebruikers- en verkeersgegevens in bijlage A en B bij artikel 13.2a Telecommunicatiewet maakt echter wel een duidelijk onderscheid.

19 Zie Odinot 2013, p. 96.

20 De Belgische rechtspraak oordeelde alvast dat Skype zich zo moest organiseren dat het bedrijf kon meewerken met een afluistermaatregel tegen een Belgische gebruiker. Skype had ingeroepen dat het door *end-to-end*-versleuteling niet kon meewerken, maar de rechtspraak volgde dat verweer niet. Die uitspraak werd bevestigd door het Hof van Cassatie: Cass. 19 februari 2019, AR P.17.1229. N.F. Verbruggen & S. Royer, 'Veroordeling Skype niet verbroken, vele vragen blijven onbeantwoord', *RW* 2018-19, 1442.

21 In België ook in het kader van een gerechtelijk onderzoek (o.l.v. de onderzoeksrechter).

22 Odinot 2013, p. 120.

23 Zie o.a. Odinot 2013, p. 129-130.

24 Odinot 2013, p. 82.

25 Odinot 2013, p. 84.

26 Odinot 2013, p. 81.

27 Ferdinandusse, Laheij & Hendriks 2015; *Kamerstukken II* 2014/15, 33870, nr. 3 (bijlage) (rapport 'de bewaarplicht telecommunicatie en de opsporing').

van elke methode achteraf niet te bepalen is.[28] Ook zonder een bewaarplicht zijn verkeersgegevens echter enige tijd beschikbaar, omdat die worden verwerkt voor factureringsdoeleinden en alle beschikbare gegevens kunnen worden gevorderd.[29] Opsporingsinstanties beargumenteren dat een minimale bewaartermijn van verkeersgegevens noodzakelijk is om te voorkomen dat de gegevens zijn verwijderd op het moment dat zij deze nodig hebben. Een gebrek aan beschikbaarheid van verkeersgegevens kan het op efficiënte wijze verzamelen van gegevens in opsporingsonderzoeken in de weg kan staan.[30]

3. HvJ EU-jurisprudentie over de bewaarplicht

De dataretentierichtlijn is omstreden vanwege de ernstige privacy-inbreuk die plaatsvindt bij het opslaan en verwerken van gegevens die veel over personen kunnen vertellen over een lange tijd, zoals 'locatiegegevens'.[31] De plek zelf, bijvoorbeeld in de nabijheid van een huisarts, kan privacygevoelig zijn, maar het is ook mogelijk om met locatiegegevens de verplaatsing van personen door de tijd heen te volgen.

De gevoeligheid bij dataretentie zit daarnaast in de algemene en ongedifferentieerde opslag van de gegevens. Dit dient het opsporingsbelang, omdat daarmee wordt verzekerd dat de gegevens beschikbaar zijn als die later nodig blijken te zijn voor een opsporingsonderzoek. Ook doemt het beeld op van 'iedereen is potentieel verdacht'[32] en vindt een privacy-inmenging plaats bij personen waarvan het overgrote deel onschuldig is. Deze aspecten worden telkens door het HvJ EU in zijn (recente) jurisprudentie over het onderwerp benadrukt.

3.1 *Digital Rights/Ierland*

In 2014 verklaarde het HvJ EU in het arrest Digital Rights/Ierland de dataretentierichtlijn in strijd met het Unierecht.[33] Meer specifiek werd de richtlijn in strijd verklaard met artikel 7 (het recht op bescherming van privacy) en artikel 8 (het recht op bescherming van persoonsgegevens) van het Handvest. Het Hof oordeelde dat de wetgever van de EU met de vaststelling van de richtlijn niet evenredig (proportioneel) heeft gehandeld in het licht van het Handvest. Al eerder verklaarden de constitutionele rechtscolleges van Bulgarije, Roemenië, Cyprus, Duitsland en Tsjechië dat de nationale wetten ter implementatie van de richtlijn geheel of gedeeltelijk onhoudbaar waren wegens strijd met privacy en andere grondrechten.[34] Toch was het arrest verstrekkend omdat het ook in andere EU-staten de ongeldigverklaring of vele rechtszaken over een bewaarplicht tot gevolg had.[35] Niet eerder werd een Europees rechtsinstrument in zijn geheel ongeldig verklaard wegens strijd met fundamentele rechten. Met dit arrest positioneerde het HvJ EU zich als een soort Europees constitutioneel hof.[36]

Het HvJ EU maakte in Digital Rights niet duidelijk in welke vorm een bewaarplicht van communicatiegegevens de toets wel kon doorstaan. De uitspraak bood weinig handvatten voor de precieze vertaalslag van deze vereisten naar het nationale niveau. Ook bleef onduidelijk of de uitspraak alleen geldt voor een strafrechtelijke context (ter bestrijding van ernstige criminaliteit) of ook in de context van nationale veiligheid.[37]

3.2 *Tele2 Sverige/Watson*

Veel lidstaten deden na het Digital Rights-arrest een beroep op de uitzondering in artikel 15 lid 1 van de e-Privacyrichtlijn om de bewaring van de communicatiegegevens via een nationale regeling toch verplicht te stellen. Geschillen over zowel de toelaatbaarheid als de inhoud van dergelijke nationale wetgeving in Zweden en in het Verenigd Koninkrijk leidden uiteindelijk tot prejudiciële vragen en een nieuw arrest over het onderwerp.[38]

In 2016 oordeelde het HvJ EU in Tele2 Sverige/Watson dat de e-Privacyrichtlijn zich verzet tegen een algemene en ongedifferentieerde bewaarplicht van communicatiegege-

28 Ferdinandusse, Laheij & Hendriks 2015, p. 36. Zie ook de kritiek op de aangehouden methodiek in het rapport van D.A.G. van Toor, 'Het doel heiligt het middel? Over de noodzaak van uniforme criteria voor evaluatie van de effectiviteit en efficiëntie van de opsporing', *PROCES* 2015, p. 229-239.

29 Zie artikel 11.5 lid 2 (Nederlandse) Telecommunicatiewet. Zie ook art. 122, § 3 (Belgische) Wet betreffende de elektronische communicatie, *BS* 20 juni 2005.

30 Zie ook, o.a., de annotatie van C. Conings in *Computerrecht* 2017/50.

31 Zie over de relatie tussen het recht op privacy en de verkeersgegevens o.a. EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, *EHRC* 2010/123, m.nt. De Hert en Van Caeneghem, par. 49-53; EHRM 8 februari 2018, 31446/12, ECLI:CE:ECHR:2018:0208JUD003144612, *EHRC* 2018/85, m.nt. M. Hagens, par. 53-54 (*Ben Faiza/Frankrijk*); HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, *EHRC* 2014/140, m.nt. M.E. Koning, par. 39 (*Digital Rights/Ierland*); HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:572 en ECLI:EU:C:2016:970, *EHRC* 2017/79, m.nt. Koning, par. 98-99 (*Tele2 Sverige AB en Watson*); EHRM 13 september 2018, 58170/13, 62322/14, 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, *Computerrecht* 2018/252, m.nt. J.J. Oerlemans, *EHRC* 2018/196, m.nt. M. Hagens, par. 356 (*Big Brother Watch e.a./het Verenigd Koninkrijk*), HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, par. 117 (*La Quadrature du Net e.a./Premier ministre e.a.*) en HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, r.o. 36-37 (*H.K./Prokuratuur*).

32 N. Falot & H. Hijmans, 'Tele2: de afweging tussen privacy en veiligheid nader omlijnd. Een tweede arrest over de bewaarplicht van telecommunicatiegegevens in het Europees recht', *NtEr* 2017, nr. 3, p. 48 (hierna: Falot & Hijmans 2017).

33 HvJ EU 8 april 2014, C-293/12, C-594/12, ECLI:EU:C:2014:238, *EHRC* 2014/140, m.nt. M.E. Koning (*Digital Rights/Ierland*).

34 Zie G-J. Zwenne & F. Simons, 'Duitse bewaarplicht ongrondwettig. En in Nederland?', *IR* 2010, nr. 3.

35 Voor in Nederland: Rb. Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498 en paragraaf 5. Zie voor in België, waar het Grondwettelijk Hof bijna letterlijk de overwegingen van het Hof van Justitie kopieerde: C. Conings & F. Verbruggen, 'Grondwettelijk Hof plaatst reparateurs dataretentiewet voor moeilijke opdracht', *Juristenkrant* 2015, afl. 312, 1-2 en paragraaf 6.

36 Falot & Hijmans 2017, p. 45.

37 Zie, o a., M. Hagens & C.M.J. Ryngaert, 'Massasurveillance en privacy: De betekenis van het EHRM-arrest Big Brother Watch e.a. t. het Verenigd Koninkrijk voor het EU-recht', *Tijdschrift voor Internetrecht* 2018, nr. 5/6, p. 216-217 (hierna: Hagens & Ryngaert 2018).

38 Zie ook Falot & Hijmans 2017.

vens voor aanbieders van elektronische communicatieaanbieders ter bestrijding van (ernstige) criminaliteit.[39] Ook een nationale regeling met een algemene en ongedifferentieerde bewaring van alle verkeersgegevens van alle abonnees en geregistreerde gebruikers is disproportioneel in het licht van het recht op privacy en betreft een regeling die verder gaat dan strikt noodzakelijk is in een democratische rechtsorde.[40]

3.3 *Privacy International en La Quadrature du Net e.a.*

In 2020 bestendigde het HvJ EU in de arresten Privacy International en La Quadrature du Net e.a. het oordeel dat een algemene en ongedifferentieerde bewaarplicht van verkeersgegevens of de ongedifferentieerde doorzending (in real time) van deze gegevens disproportioneel en in strijd is met de e-Privacyrichtlijn en het Handvest.[41]

De arresten Privacy International en La Quadrature du Net e.a. zijn naast de overwegingen over de bewaarplicht en de doorzending van communicatiegegevens ook erg interessant, omdat het HvJ EU uitspraken doet over de rechtmatigheid van nationale maatregelen die door lidstaten worden genomen ter bescherming van de nationale veiligheid. Dat is niet vanzelfsprekend, omdat de bescherming van de nationale veiligheid in artikel 4 lid 2 van het oprichtingsverdrag van de EU (VEU) de 'uitsluitende verantwoordelijkheid van de lidstaten' wordt genoemd. De e-Privacyrichtlijn en het Handvest zijn echter van toepassing omdat bij dataretentie en het doorzenden van communicatiegegevens door aanbieders van elektronische communicatiediensten op basis van vooraf vastgestelde parameters, sprake is van een verwerking van gegevens in de zin van de e-Privacyrichtlijn.[42] Een beroep op de uitzondering in artikel 15 e-Privacyrichtlijn mag niet de achterliggende bescherming van de Europese regelgeving uithollen.[43]

In de proportionaliteitstoets gaat het HvJ EU steeds na of de ernst van de inmenging op de fundamentele rechten die wordt veroorzaakt door de bewaarplicht als maatregel evenredig is aan het algemeen belang dat wordt nagestreefd. Voor de afweging met het algemeen belang valt op dat het HvJ EU deze in La Quadrature du Net e.a. duidelijk rangschikt, waarbij de bescherming van de nationale veiligheid als het hoogste belang wordt gezien, daarna de bestrijding van ernstige criminaliteit, vervolgens de bestrijding van ernstige criminaliteit en ten slotte de bescherming van de openbare veiligheid.[44]

Ter bescherming van de nationale veiligheid zijn de meest verstrekkende maatregelen mogelijk. Hierbij moet de nationale wetgeving van de lidstaten telkens duidelijke en precieze regels bevatten die de reikwijdte en de toepassing van de maatregel in kwestie uiteenzetten, en minimumwaarborgen opleggen, zodat de personen van wie de persoonsgegevens worden bewaard voldoende waarborgen hebben dat de gegevens effectief worden beschermd tegen het risico op misbruik.[45] Het HvJ EU acht een verplichting alle communicatiegegevens vooraf te bewaren alleen mogelijk bij een 'serieuze dreiging voor de nationale veiligheid'[46] voor zover deze reëel en actueel of voorzienbaar is.[47] Een dergelijke bewaarplicht is slechts mogelijk voor een (zo kort mogelijke) bepaalde periode (met de mogelijkheid tot verlenging).[48] Ook moeten er waarborgen tegen misbruik in nationale wetgeving bestaan, waaronder de controle door een rechterlijke instantie of onafhankelijke administratieve instantie met bindende bevoegdheden.[49]

Het blijft voor ons echter onduidelijk wat wordt verstaan onder een 'serieuze dreiging voor de nationale veiligheid die reëel, actueel of voorzienbaar is'. Het HvJ EU gaat hier niet nader op in. Gaat het daarbij enkel om een reële dreiging van een (terroristische) aanslag, wat het HvJ EU als voorbeeld noemt, of ook om een cybersecurity-incident dat de economie dreigt te ontwrichten of valt hier meer onder, zoals het beschermen van de nationale veiligheid tegen contraspionage door buitenlandse inlichtingenofficieren? Het is onwenselijk dat het HvJ EU hier onduidelijk over blijft.

4. De bewaarplicht ter bestrijding van criminaliteit

De preventieve bewaring van verkeers- en locatiegegevens van gebruikers van communicatiediensten is volgens het HvJ EU slechts onder strikte voorwaarden mogelijk voor de vervolging van ernstige criminaliteit of voor de bescherming voor de openbare veiligheid. Een algemene en ongedifferentieerde bewaarplicht is in het kader van de

39 HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB/Post-och telestyrelsen en Secretary of State of the Home Department/Watson*), *Computerrecht* 2017/50, m.nt. C. Conings, *EHRC* 2017/79, m.nt. M.E. Koning.

40 HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 SverigeAB/Watson*), par. 112 en 107.

41 Zie ook S. Careel & S. Royer, 'Bewaart het Hof van Justitie evenwicht tussen veiligheid en privacy in nieuwe dataretentie-arresten?', *P&I* 2020/6, p. 269-272 (hierna Careel & Royer 2020) en *EHRC Updates* 2020/253, m.nt. J. Schoers.

42 Zie *Privacy International*, par. 39, 41 en *La Quadrature du Net e.a.*, par. 93, 95, 96, 104.

43 *La Quadrature du Net e.a.*, par. 99 en *Privacy International*, par. 44. Zie hierover verder de annotatie bij de arresten van Oerlemans en Hagens in *JBP* 2021/1. Zie over de relatie tussen het Hof van Justitie en nationale veiligheid ook Hagens & Ryngaert 2018.

44 Zie *La Quadrature du Net e.a.*, par. 136.

45 Zie ook de annotatie van J. Schoers bij *La Quadrature du Net e.a.* in *EHRC-Updates* 2021.

46 *La Quadrature du Net e.a.*, par. 135 ('activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities').

47 *La Quadrature du Net e.a.*, par. 137 ('genuine and present or forseeable'). Zie ook Careel & Royer 2020, p. 271.

48 *La Quadrature de Net e.a.*, par. 137-138.

49 *La Quadrature du Net e.a.*, par. 139.

bestrijding van ernstige criminaliteit dus niet mogelijk, maar een bewaarplicht van bepaalde communicatiegegevens is wel mogelijk voor zover beperkt in tijd, soort, hoeveelheid en plaats, en ter bestrijding van ernstige criminaliteit. Een dergelijk bevel tot het bewaren van deze gegevens (gevolgd door een vordering van de gegevens), moet volgens het HvJ EU tot het strikt noodzakelijke worden beperkt, bijvoorbeeld in tijd en tot een kring van personen.[50]

Het is volgens het HvJ EU ook mogelijk een bewaarplicht in te stellen met een geografische afbakening. Het Hof licht toe dat het daarbij kan gaan om plaatsen waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plaatsen of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plaatsen, zoals vliegvelden, stations of tolzones.[51] Het Nederlandse evaluatierapport over de bewaarplicht biedt mogelijk een meer concreet voorbeeld. Daarin wordt beschreven dat het opvragen van verkeersgegevens mogelijk is op basis van alle mobiele telefoons die in het opgevraagde tijdsbestek zijn gebeld, zelf hebben getelefoneerd of connectie hebben gehad met het internet via een specifieke mastlocatie.[52] Om zendmastgegevens op te kunnen vragen, moet er sprake zijn van een verdenking van een ernstig misdrijf. Deze zendmastgegevens worden meestal gevorderd bij seriematige delicten. In dat geval worden de gegevens van verschillende locaties met elkaar vergeleken, in de hoop een terugkerend nummer te kunnen identificeren.[53]

Vanwege de abstracte criteria van het HvJ EU ter beperking van een bewaarplicht zullen EU-lidstaten voor zichzelf moeten nagaan of hun wetgeving aan deze kwalitatieve vereisten voldoet. In Nederland wordt bijvoorbeeld voor het begrip 'ernstig misdrijf' vaak de categorie misdrijven in artikel 67 Sv aangehouden, op basis waarvan personen in voorlopige hechtenis mogen worden gesteld. In België bevat het Wetboek van Strafvordering dan weer een lijst van ernstige misdrijven die vergaande onderzoeksmaatregelen rechtvaardigen. Die lijst telt ondertussen al 45 misdrijven en lijkt dus geen goede richtlijn meer voor wat precies ernstige criminaliteit is.[54] Het is niet duidelijk of het HvJ EU aan zwaardere misdrijven denkt, bijvoorbeeld misdrijven op basis waarvan een gevangenisstraf van vier jaar of meer staat. Wetgevers van EU-lidstaten zullen dat voor zichzelf moeten nagaan. De arresten zijn vast niet het laatste woord voor de lidstaten.

Er is nog aantal prejudiciële vragen over vergelijkbare vraagstukken aanhangig bij het HvJ EU, waarbij we niet uitsluiten dat er nog meer komen.[55]

Ten slotte staat het HvJ EU in La Quadrature du Net e.a. meer toe met betrekking tot de bewaring van gebruikersgegevens. In dit arrest overweegt het Hof meer specifiek dat de privacy-inbreuk kleiner is bij het bewaren van gebruikersgegevens, waaronder IP-adressen van de oorsprong van communicatie en identificatiegegevens van gebruikers van elektronische communicatiediensten, in vergelijking met andere verkeers- en locatiegegevens.[56] Een wettelijke maatregel die voorziet in een algemene en ongedifferentieerde bewaarplicht van gebruikersgegevens (waaronder het toegewezen IP-adres aan gebruikers) ter bestrijding van ernstige criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid, is volgens het HvJ EU mogelijk.[57] De bewaartermijn van deze gebruikersgegevens mag niet langer zijn dan wat strikt noodzakelijk is in het licht van het nagestreefde doel. Het HvJ EU stelt daarbij geen maximale termijn. De regels die dat mogelijk maken moeten in nationale wetgeving worden gevat, waarbij de betrokken personen beschikken over waarborgen tegen het risico van misbruik.[58] Het HvJ EU concretiseert niet wat deze maatregelen zijn, maar gedacht kan worden aan de toepassing van wet- en regelgeving over de verwerking van persoonsgegevens en een effectieve controle daarop.

De belangrijke nuancering en wijziging ten opzichte van de voorgaande jurisprudentie op basis waarvan een bewaarplicht van gebruikersgegevens voor de bestrijding van ernstige criminaliteit mogelijk is, is voor de praktijk heel belangrijk. In opsporingsonderzoeken naar cybercriminaliteit leidt het spoor vaak naar internetaanbieders in andere landen, waar de dader zich bevindt en gebruikmaakt van een internetverbinding. Het opvragen van gebruikersgegevens om personen te identificeren aan wie een IP-adres is toegewezen, is daarbij een belangrijke opsporingsmethode (zie paragraaf 2.1).[59] Het arrest geeft lidstaten het vertrouwen dat een dergelijke bewaarplicht ten aanzien van gebruikersgegevens mogelijk is. Ook in andere strafzaken (naar bijvoorbeeld stalking, opruiing of smaad) kunnen gebruikersgegevens bewijs opleveren over wie bijvoorbeeld op welk moment van een OTT-dienst gebruik heeft gemaakt, als een bewaarplicht ook naar die diensten wordt uitgebreid (zie paragraaf 2.2).

50 *La Quadrature du Net e.a.*, par. 144 en par. 147-149.
51 *La Quadrature du Net e.a.*, par. 149. Zie ook Careel & Royer 2020, p. 270.
52 Odinot e.a. 2013, p. 20.
53 Idem. Zie ook voorbeeld van liquidatiezaken in Antwerpen en Amsterdam in het rapport van Ferdinandusse e.a. 2015, p. 9 met verwijzing naar Rb. Amsterdam 1 december 2014, ECLI:NL:RBAMS:2014:8047.
54 Art. 90*ter*, §§ 2-4 Belgische Wetboek van Strafvordering. Zie hierover W. Yperman, S. Royer & F. Verbruggen, 'Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering', *NC* 2019, (389) 398.
55 Zie tot dusver het verzoek van 25 maart 2020, *Commissioner of the Garda Síochána e.a./Ierland*, C-140/20; verzoeken van 29 oktober 2019, *Spacenet & Telekom Deutschland/Duitsland*, C-793/19 en C-794/19.
56 *La Quadrature du Net e.a.*, par. 152 en 157. Zie in vergelijkbare zin over de ernst van de privacy-inbreuk EHRM 30 januari 2020, nr. 50001/12, ECLI:CE:ECHR:2020:0130JUD005000112 par. 92 en 94 (*Breyer/Duitsland*) en HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, r.o. 34 (*H.K./Prokuratuur*).
57 *La Quadrature du Net e.a.*, par. 155-159.
58 *La Quadrature du Net e.a.*, par. 168.
59 Zie ook *La Quadrature du Net e.a.*, par. 154.

Alles overziend is de bewaarplicht zoals het oorspronkelijk bedoeld was, algemeen en ongedifferentieerd, dus alleen nog voor gebruikersgegevens mogelijk. Op basis van deze conclusie verdient het aanbeveling dat de Europese Commissie de invoering van een bewaarplicht op Europees niveau heroverweegt, om verschillen in de beschikbaarheid van bepaalde gegevens ter bestrijding van ernstige criminaliteit weg te nemen.

5. Gevolgen voor Nederland

In Nederland was de dataretentierichtlijn (2006/24/EG) geïmplementeerd in de Wet bewaarplicht telecommunicatiegegevens uit 2009.[60] De wet regelde een algemene bewaarplicht voor gebruikers- en verkeersgegevens met een bewaartermijn in artikel 13.2a van de Telecommunicatiewet. De gegevens moesten worden bewaard voor een periode van twaalf maanden voor gegevens in verband met telefonie en zes maanden voor internetgegevens.

Naar aanleiding van het arrest Digital Rights van het HvJ EU in 2014, waarin de dataretentierichtlijn ongeldig is verklaard, is ook in Nederland een kort geding gestart om de wetgeving onrechtmatig te verklaren. Op 11 maart 2015 verklaarde een Haagse voorzieningenrechter de bewaarplicht onrechtmatig en stelde deze buiten werking.[61] Volgens de rechter was de inbreuk die de wet maakte op de in de artikelen 7 en 8 van het EU-Handvest beschermde rechten niet beperkt tot het strikt noodzakelijke en daarmee ontoelaatbaar. Het probleem lag volgens de voorzieningenrechter in de omstandigheid dat de wet onvoldoende waarborgen bood, zoals bij de toegang tot de bewaarde gegevens, niet dat een ruime bewaarplicht hoe dan ook niet evenredig was met het beoogde doel van opsporing van ernstige criminaliteit.

De uitspraak sterkte de regering in haar standpunt dat een algemene bewaarplicht noodzakelijk was voor de bestrijding van ernstige criminaliteit, maar met meer waarborgen zoals onafhankelijke toestemming voor toegang tot de gegevens. In september 2016 volgde een nieuw wetsvoorstel voor het bewaren van verkeersgegevens.[62] In het nader rapport van het wetsvoorstel gaf de regering aan dat een prejudiciële vraag (Tele2/Watson) aanhangig was bij het HvJ EU over de vraag of een algemene bewaarplicht als zodanig onevenredig is met het Unierecht.

Uiteindelijk leidde de regering uit het arrest Tele2/Watson (uit december 2016) af dat ingrijpende aanpassingen van de wijzigingswet voor de bewaring van telecommunicatiegegevens nodig waren.[63] De in het wetsvoorstel opgenomen verplichting tot het bewaren van verkeers- en locatiegegevens zou worden beperkt tot een regeling met betrekking tot uitsluitend (alle) gebruikersgegevens. Daarbij was ook een verplichting voor ogen dergelijke gegevens beschikbaar te houden om te kunnen voldoen aan een vordering om de gegevens te herleiden van een gebruiker van een telecommunicatiedienst of -netwerk op een bepaald tijdstip.[64]

Sinds maart 2018 ligt het wetstraject echter stil. Er is nog geen aangepast wetsvoorstel ingediend. Ondertussen zijn de resultaten van het onderzoek naar de mogelijkheden voor identificatie op internet op basis van IP-adres gepubliceerd[65] en de beleidsopties bekend om identificatie van gebruikers op basis van IP-adres beter mogelijk te maken (zie paragraaf 2.1). De implementatie van de Telecomcode (zie paragraaf 2.2) roept ook de vraag op of een eventuele bewaarplicht van gebruikersgegevens ter bestrijding van ernstige criminaliteit zou moeten worden uitgebreid naar OTT-diensten.

Op basis van de analyse van het arrest La Quadrature du Net e.a. bestaat er volgens ons de mogelijkheid voor een bewaarplicht van gebruikersgegevens voor aanbieders van elektronische communicatiediensten en -netwerken in Nederland. De Europese jurisprudentie staat niet in de weg van een verdere behandeling van een aangepast wetsvoorstel in de Tweede Kamer en de Eerste Kamer. De noodzaak van de beschikbaarheid van deze gebruikersgegevens ter bestrijding van ernstige criminaliteit en ter bescherming van de nationale veiligheid – iets waar wij overigens niet aan twijfelen – lijkt de aanpassingswet in combinatie met noodzakelijke aanpassingen in de Telecommunicatiewet toch enigszins urgent te maken.

6. Gevolgen voor België

In België zitten de wetsbepalingen over dataretentie verspreid in de Wet betreffende de elektronische communicatie (hierna: WEC),[66] die de bewaartermijnen vastlegt, en in het Wetboek van Strafvordering (hierna: Sv.), dat de voorwaarden voor toegang tot de gegevens bepaalt. Dat wettelijk kader onderging al meerdere wijzigingen.

60 *Stb.* 2009, 333.

61 Rb. Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498, *Computerrecht* 2015/88, m.nt. F.C. van der Jagt.

62 *Kamerstukken II* 2015/16, 34537, nr. 2 (Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken (aanpassing bewaarplicht telecommunicatiegegevens)). Zie over het wetsvoorstel ook A.C. Diesfeldt & F.C.W. de Graaf, 'Dataretentie. Een kwestie van alles of niets?', *NJB* 2015/592, p. 740-747.

63 Kamerbrief van 25 september 2018 over de aanpassing bewaarplicht telecommunicatiegegevens (*Kamerstukken II* 2017/18, 34537, nr. 7).

64 Kamerbrief van 25 september 2018 over de aanpassing bewaarplicht telecommunicatiegegevens (*Kamerstukken II* 2017/18, 34537, nr. 7).

65 *Kamerstukken II* 2017/18, 34537, nr. 8. Zie ook het rapport Van der Vorst e.a. 2019.

66 *BS* 13 juni 2005.

De oorspronkelijk ongedifferentieerde bewaarplicht[67] kreeg in 2013 een duidelijke wettelijke grondslag.[68] Zo moesten verkeers- en locatiegegevens en identificatiegegevens twaalf maanden worden bewaard, maar een koninklijk besluit kon die termijn verlengen voor bepaalde categorieën van gegevens, bijvoorbeeld in het geval van een terroristische aanslag.[69] De inhoud van communicatie mocht in geen geval worden bewaard.[70] In navolging van de vernietiging van de dataretentierichtlijn (supra) vernietigde ook het Grondwettelijk Hof de dataretentiewet van 2013.[71] Hierop kroop de wetgever opnieuw in de pen en dit leidde in 2016 tot een nieuwe dataretentiewet.[72] Een a priori-differentiatie van te bewaren gegevens op grond van personen, periodes of geografische zones, achtte de wetgever niet mogelijk.[73] Een a priori differentiatie voor bepaalde beroepsgroepen is volgens de wetgever evenmin mogelijk, een verhoogde bescherming wel.[74]

De huidige regeling is van toepassing op aanbieders van openbare telefoniediensten en op operatoren van openbare elektronische communicatienetwerken. De wet maakt een verschil tussen identificatiegegevens, verbindings- en lokalisatiegegevens en persoonlijke communicatiegegevens,[75] maar acht een bewaringsperiode van twaalf maanden voor elk van die categorieën noodzakelijk.[76] Die termijn loopt vanaf het moment waarop communicatie via de gebruikte dienst voor de laatste keer mogelijk is.[77]

In het kader van criminaliteitsbestrijding hebben gerechtelijke autoriteiten onder bepaalde voorwaarden toegang tot identificatie- en verkeersgegevens. De differentiatie in de toegang tot de bewaarde gegevens hangt af van een objectief criterium, namelijk de ernst van de feiten. Identificatiegegevens voor de lichtste misdrijven kunnen slechts voor een periode van zes maanden voorafgaand aan de beslissing van de procureur des Konings worden opgevraagd.[78] De onderzoeksrechter en uitzonderlijk de procureur des Konings[79] kunnen verkeers- en locatiegegevens slechts opvragen als de feiten minstens een gevangenisstraf van een jaar tot gevolg kunnen hebben (proportionaliteitsvereiste).[80] Hoewel alle gegevens twaalf maanden worden bewaard, kan de onderzoeksrechter ze niet tijdens die hele periode opvragen. De maatregel kan niet bevolen worden voor de lichtste misdrijven, strafbaar met minder dan één jaar gevangenisstraf. Voor misdrijven strafbaar met één tot vijf jaren gevangenisstraf kan 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 twaalf maanden.[81]

Hoewel de Belgische dataretentiewet dus verscherpte waarborgen bevatte, werd ze na het Tele2 Sverige arrest van het HvJ EU (supra) opnieuw het voorwerp van een vernietigingsberoep voor het Grondwettelijk Hof.[82] In een arrest van 19 juli 2018 meende dit Hof geen uitspraak te kunnen doen, nu er twee zaken over dezelfde problematiek hangende waren bij het HvJ EU.[83] Aangezien vele lidstaten moeilijkheden ondervinden om hun dataretentiewetgeving op de rechtspraak van het HvJ EU af te stemmen, achtte het Grondwettelijk Hof het noodzakelijk een drievoudige vraag aan het HvJ EU te stellen, die leidde tot het arrest La Quadrature du Net e.a.[84] In zijn vraagstelling verwees het Grondwettelijk Hof onder meer naar de positieve verplichtingen van de lidstaten op grond van de artikelen 3 en 8 EVRM.[85] Zo volgt uit het arrest van het EHRM in K.U./Finland dat lidstaten in een wettelijk kader moeten voorzien dat de effectieve bestraffing van seksueel misbruik van minderjarigen en de identificatie van daders die elektronische communicatienetwerken gebruiken, mogelijk maakt.[86]

Uit de lezing van La Quadrature du Net e.a. blijkt duidelijk dat een algemene bewaarplicht van verkeersgegevens zoals die vandaag in België bestaat, niet te verzoenen valt met het oordeel van het HvJ EU. Er volgt dus heel waarschijnlijk minstens een gedeeltelijke vernietiging van de Belgische dataretentiewet uit 2016.[87] De wetgever zal dan

67 Oud art. 126 WEC.

68 Wet van 30 juli 2013, houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van Strafvordering (1), *BS* 20 augustus 2013.

69 Oud art. 126, § 4 WEC.

70 Art. 126, § 1, lid 5 WEC.

71 GwH 11 juni 2015, 84/2015; C. Conings & F. Verbruggen, 'Grondwettelijk Hof plaatst reparateurs dataretentiewet voor moeilijke opdracht', *Juristenkrant* 2015, afl. 312, 1-2.

72 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.

73 "*Met betrekking tot de verwijzing naar een 'geografische zone' of een 'kring van personen' zou een activering van artikel 126 WEC op grond van dit type criterium op profilering lijken, met de risico's van discriminatie die eruit voortvloeien.*" Wetsontwerp van 11 januari 2016, *Parl. St.* Kamer 2015-16, nr. 54-1567/001, 10 e.v.

74 Wetsontwerp van 11 januari 2016, *Parl. St.* Kamer 2015-16, nr. 54-1567/001, 12.

75 Bijvoorbeeld respectievelijk wie de houder is van een gsm-nummer, van waar een oproep is gebeurd en wie met wie gebeld heeft. Wetsontwerp van 11 januari 2016, *Parl. St.* Kamer 2015-16, nr. 54-1567/001, 13.

76 Art. 126, § 3 WEC.

77 Wetsontwerp van 11 januari 2016, *Parl. St.* Kamer 2015-16, nr. 54-1567/001, 27.

78 Dit zijn feiten die geen correctionele gevangenisstraf van minstens één jaar tot gevolg kunnen hebben. Art. 46*bis*, § 1, lid 5 Sv.; wetsontwerp van 11 januari 2016, *Parl. St.* Kamer 2015-16, nr. 54-1567/001, 38.

79 O.a. bij ontdekking op heterdaad van een feit bedoeld in art. 90*ter*, § 2-4 Sv. (art. 88*bis*, § 1, lid 5-8 Sv.).

80 Art. 88*bis*, § 1, lid 1 Sv.: wetsontwerp van 11 januari 2016, *Parl. St.* Kamer 2015-16, nr. 54-1567/001, 40 e.v.

81 Art. 88*bis*, § 2 Sv.; wetsontwerp van 11 januari 2016, *Parl. St.* Kamer 2015-16, nr. 54-1567/001, 40 e.v.

82 GwH 19 juli 2018, 96/2018.

83 GwH 19 juli 2018, 96/2018, B.17.1 en B.17.2.

84 GwH 19 juli 2018, 96/2018, B.21.

85 GwH 19 juli 2018, 96/2018, B.22.

86 EHRM 2 december 2008, 2872/02, ECLI:CE:ECHR:2008:1202JUD000287202.

87 S. Royer & S. Careel, 'Houdbaarheidsdatum algemene dataretentie voor criminaliteitsbestrijding is verstreken', *Juristenkrant* 2020, afl. 416, 1-2.

terug aan zet komen om de verschillende opdelingen die het HvJ EU maakt, om te zetten in het nationale recht. Dat zal geen eenvoudige klus zijn. Zo blijft het nog steeds onduidelijk hoe de bewaarregeling van verkeersgegevens kan worden gedifferentieerd op grond van personen, zonder discriminatoir te zijn.

7. Conclusie

In dit artikel zijn wij nagegaan wat de gevolgen zijn van het arrest La Quadrature du Net e.a. van het HvJ EU voor een bewaarplicht als maatregel ter bestrijding van ernstige criminaliteit in Nederland en België. De belangrijkste conclusie van het arrest is dat het HvJ EU ruimte biedt voor een bewaarplicht van gebruikersgegevens bij aanbieders van elektronische communicatiediensten en een preventief bewaren van verkeersgegeven beperkt mogelijk maakt ter bestrijding van ernstige criminaliteit. De verwerking van verkeersgegevens en in het bijzonder locatiegegevens is dermate gevoelig dat het HvJ EU een algemene en ongedifferentieerde verplichting tot bewaring ter bestrijding van ernstige criminaliteit als disproportioneel beschouwt. Een preventieve bewaring van verkeersgegevens ter bestrijding van ernstige criminaliteit moet daarom beperkt zijn, bijvoorbeeld in duur, kring van personen, en/of met een geografische afbakening. Ten slotte biedt het HvJ EU enige ruimte voor een bewaarplicht bij bedreigingen voor de nationale veiligheid, voor zover deze reëel en actueel of voorzienbaar is.

In Nederland ligt de behandeling van een nieuw wetsvoorstel voor een bewaarplicht sinds 2018 stil. Uit de voorbereiding van het voorstel voor de invoering van een bewaarplicht in Nederland blijkt dat zich technische uitdagingen voordoen bij het op effectieve wijze koppelen van de gebruikers van telecommunicatiediensten aan een apparaat, maar dat die niet onoverkomelijk zijn. Voor een bewaarplicht van gebruikersgegevens in Nederland is voor de bestrijding van met name cybercriminaliteit veel te zeggen. Ook verdient een uitbreiding van een bewaarplicht van gebruikersgegevens bij OTT-diensten overweging, hoewel daarbij onvermijdelijk handhavingsproblemen ontstaan. Het arrest van het HvJ EU biedt in die zin Nederland meer vertrouwen dat een bewaarplicht van gebruikersgegevens voor aanbieders van communicatiediensten voldoet aan de vereisten van het HvJ EU.

In België maakt La Quadrature du Net e.a. duidelijk dat een algemene bewaarplicht van verkeersgegevens zoals die vandaag de dag in België bestaat, niet te verzoenen valt met het oordeel van het HvJ EU. Er volgt dus heel waarschijnlijk minstens een gedeeltelijke vernietiging van de Belgische dataretentiewet uit 2016. De wetgever zal dan opnieuw aan zet komen om de verschillende opdelingen die het HvJ EU maakt, om te zetten in het nationale recht.

Gezien het aantal staten dat zich heeft aangesloten bij de prejudiciële vragen en het aantal prejudiciële vragen dat gerelateerd is aan het onderwerp, ligt dat staten nauw aan het hart. Ze zien in een bewaarplicht klaarblijkelijk een belangrijk instrument voor de bescherming van de nationale veiligheid, als maatregel ter bestrijding van ernstige criminaliteit en voor de bescherming van de openbare orde. In dit artikel wordt Nederlands onderzoek aangehaald dat de noodzaak van een bewaarplicht van gebruikersgegevens aantoont en het nut van de bewaring van verkeersgegevens ten behoeve van de opsporing.

Het bovenstaande in aanmerking genomen, valt ook veel te zeggen voor de herintroductie van een bewaarplicht van gebruikersgegevens op Europees niveau. Het voorkomt fragmentering van de regelgeving, waardoor het in de ene lidstaat bijvoorbeeld wel mogelijk is gebruikers te identificeren, maar in een andere niet. Criminaliteit laat zich niet door grenzen tegenhouden en dat geldt zeker voor cybercriminaliteit.