HET MOEILIJKE EVENWICHT TUSSEN PRIVACY & VEILIGHEID:

De impact van het debat over het bewaren van communicatiegegevens

De rechtspraak van het Hof van Justitie beperkte de mogelijkheden voor nationale lidstaten om communicatiegegevens bij te houden voor de strijd tegen ernstige criminaliteiten en de bescherming van de nationale veiligheid. Binnen deze richtlijnen proberen nationale regelgevers, met inbegrip van de Belgische wetgever, een regeling uit te dokteren die het gebruik van deze gegevens veiligstelt voor vervolgende autoriteiten en inlichtingendiensten. Deze bijdrage duidt hoe de Europese rechtspraak tot een lappendeken aan dataretentiebeleid in de Europese Unie zorgde, wat grensoverschrijdende samenwerking bemoeilijkt. De auteur beargumenteert dat transparante cijfers over de nationale regels van dataretentie en het gebruik van communicatiedata van groot belang voor het debat en coherentie kunnen zijn.

Sleutelwoorden:

Dataretentie;
Privacy;
bescherming van persoonsgegevens;
surveillance;
Europese rechtspraak;
Antigoon;
openbare veiligheid;
ernstige criminaliteit.

Ass. Prof. Catherine Van de Heyning *(Faculty of Law, University of Antwerp, promotor BELSPO @ntidote-project)*

Inleiding

Telkens we op het internet gaan, via een app een bericht sturen of bellen, tikken, toetsen en browsen, creëren we nieuwe data over ons communicatie – en surfgedrag. Deze data worden bijgehouden en verwerkt door operatoren en dienstverleners van elektronische communicatienetwerken. De inhoud van onze communicatie wordt niet bewaard omdat dit zou botsen op de vertrouwelijkheid van communicatie. Daarentegen kan deze bewaring wel voor de metadata van onze communicatie: van waar, met wie, hoe lang en wanneer we in contact waren met anderen, of nog, de pagina's die we bezochten, hoe lang we op die pagina bleven en van waaruit we connecteerden. Deze metadata bevatten veel informatie over ons privéleven. De bewaring van deze data kan bovendien gevaarlijk zijn als ze in de verkeerde handen vallen. Bijvoorbeeld kunnen die data de locatie verraden van een gezochte oppositieleider in een autocratisch systeem. Of nog, indien deze data gelekt worden, kunnen deze gegevens misbruikt worden door cybercriminelen voor succesvolle en overtuigende phishing-operaties waarbij onze eigen informatie tegen ons wordt gebruikt. Metadata zijn niet onschuldig en worden dan ook beschermd door het recht op privacy en de bescherming van persoonsgegevens. Dat betekent dat elke bewaring van deze gegevens, toegang tot deze gegevens of het gebruik van deze gegevens slechts mogelijk is op basis van een wettelijke basis, voor een legitieme doelstelling en in zover dit gebruik in verhouding staat tot de doelstelling die werd nagestreefd.

De Europese Unie regelde met de E-privacyrichtlijn[1] de bescherming van deze met-

1 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), Jur. L-201, 0037 – 0047. Hierna "e-privacy richtlijn".

adata, in het bijzonder de gegevens die het mogelijk maken ons te identificeren (identificatiegegevens), onze locatie te kennen (locatiegegevens) en de tijd, duur en tijdstip van onze communicatie weergeeft (verkeersgegevens). Deze richtlijn hanteert het principe dat communicatiegegevens niet bewaard mogen worden, tenzij voor bepaalde legitieme doelstellingen, zoals het onderhoud van het digitale communicatienetwerk. De vraag in welke mate deze gegevens ook bewaard moeten worden voor de strijd tegen ernstige criminaliteit en voor de bescherming van de nationale veiligheid beroert in de Europese Unie al jarenlang de gemoederen. Toen het Hof van Justitie in 2014 de Europese richtlijn voor dataretentie[2] neersabelde en meegaf dat het bewaren van locatie – en verkeersgegevens van de hele bevolking in strijd is met de fundamentele rechten van de bescherming van privacy en persoonsgegevens, kwam er veel kritiek van nationale vervolgende autoriteiten en inlichtingendiensten.[3] Zonder deze data, zo beweerden ze, zou de strijd tegen criminaliteit en de bescherming van de nationale veiligheid ernstig ondermijnd worden.

Wat volgde was een 'heen en weer' aan prejudiciële vragen tussen de hoogste nationale rechtscolleges en het Hof van Justitie waarbij het Hof een balans probeerde te vinden tussen enerzijds de bescherming van fundamentele rechten en anderzijds de bescherming van de nationale veiligheid en strijd tegen criminaliteit. De Belgische wet[4] die dataretentie mogelijk maakt voor de strijd tegen criminaliteit, werd in 2021 vernietigd door het Grondwettelijk Hof,[5] waarna de regering in maart 2022 een nieuwe ontwerp van wet in het Belgische parlement introduceerde. Opnieuw is dit wetsontwerp voer voor hevige discussie en – in welke vorm het ook gestemd wordt – zal de toekomstige wet zonder twijfel opnieuw voorgelegd worden aan de hoogste nationale en Europese rechtscolleges.

Deze bijdrage focust op de vraag waar het evenwicht tussen privacy en de bescherming van persoonsgegevens enerzijds en veiligheid en de bestrijding van criminaliteit vandaag ligt en wat de impact op de korte termijn zal zijn voor de bestrijding van criminaliteit en bescherming van de nationale veiligheid. Een eerste deel bespreekt de principes die het Hof van Justitie over het gebruik van dataretentie vastlegde en welke rol dataretentie vandaag in België speelt. In een tweede deel wordt meer in detail ingegaan op de huidige regels over het bewaren, de toegang en gebruik van elektronische communicatiegegevens zoals vastgelegd door het Hof van Justitie. Een derde deel verlegt de focus naar België en bekijkt enerzijds hoe de Belgische rechtspraak de Luxemburgse dataretentie-principes toepast en anderzijds hoe het nieuwe wetsontwerp deze principes in concrete wetgeving probeert om te zetten. In een vierde en laatste deel volgt het huidige evenwicht tussen privacy en veiligheid alsook de impact van de nationale toepassing van deze regels op het strafonderzoek in Europa op de korte termijn. Deze bijdrage besluit dat het Hof van Justitie een evenwicht heeft proberen te vinden waarbij het zowel privacy – als veiligheidsbesognes ernstig in overweging nam, maar wat momenteel resulteert in incoherentie in de aanpak tussen de nationale lidstaten wat samenwerking bemoeilijkt. Deze bijdrage beargumenteert dat het debat gewonnen zou zijn met transparantie over het gebruik van communicatiegegevens in strafonderzoeken.

2 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, Jur. L-105, 54–63. Hierna "dataretentierichtlijn".

3 Over de impact zie: Maria Murphy, "Data retention in the aftermath of Digital Rights Ireland and Seitlinger", Irish Criminal Law Journal, vol. 24, nr. 4 (2014): 105; Niklas Vainio en Samuli Miettinen, "Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States", *International Journal of Law and Information Technology*, vol. 23, nr. 3 (2015): 290–309.

4 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, 44717. Hierna: dataretentiewet 2016.

5 GwH 22 april 2021, nr. 57/2021. Te raadplegen: www.const-court.be.

De grondslagen van dataretentie: de regels en het gebruik

De opbouw en afbraak van Europese dataretentieregels

In 2006 stemde de Europese Unie de dataretentierichtlijn.[6] Deze richtlijn moest de verschillende nationale regels over de bewaring van tele – en elektronische communicatie harmoniseren. Er werden drie redenen naar voorgeschoven voor deze Europese dataretentieregeling. Ten eerste meende de EU dat deze richtlijn nodig was vanuit het vrije marktdenken waarbij de Europese Unie hindernissen tussen de lidstaten verwijdert (r.o. 6). In die optiek merkte de EU op dat de vele juridische en technische verschillen in de nationale wetgeving over het bewaren van elektronische communicatiegegevens de werking van de interne markt voor elektronische communicatie bemoeilijkt. Immers, de aanbieders van elektronische communicatiediensten werden volgens de EU geconfronteerd met uiteenlopende regels van toepassing op de bewaring van identificatie - , verkeer - en locatiegegevens, en dit zowel voor de bewaringsvoorwaarden als bewaringstermijnen van communicatiegegevens. De verscheidenheid aan nationale regels werd des te problematischer met de stijgende impact van digitalisering waarbij internetoperatoren en – internetdienstenaanbieders zich niet beperken tot nationale grenzen maar hun diensten eenvoudig binnen cyberspace aanbieden. Indien elk land andere regels hanteert over welke data dan wel bijgehouden moeten worden, op welke wijze en hoe lang zou dit pan-Europese of buitenlandse spelers bemoeilijken om op een nationale markt hun digitale diensten aan te bieden.

Ten tweede had de EU reeds secundaire regelgeving uitgewerkt over de verwerking van persoonsgegevens[7] en meer specifiek over de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie[8] (hierna: E-privacy richtlijn). Deze regels concretiseren de bescherming van het privéleven en persoonsgegevens in de sector van elektronische en telecommunicatie. Het is in die context dat de Europese Unie meende dat een harmonisatie van de regels over de bewaring van elektronische en telecommunicatiegegevens nodig was voor zowel de vrije markt voor elektronische en telecommunicatie te versterken als de bescherming van de privacy en persoonsgegevens (r.o. 9).

Ten derde merkte de EU op dat deze telecommunicatiegegevens een steeds belangrijkere rol spelen in de strijd tegen criminaliteit en de bescherming van de veiligheid (r.o. 9). In de voorafgaande overwegingen van de richtlijn belichtte de EU dat de ervaring van diverse lidstaten het belang van deze verkeers- en locatiegegevens voor het onderzoeken, opsporen en vervolgen van strafbare feiten aantoonde. Hierbij werd ook verwezen naar de terroristische dreiging waarbij het belang van dergelijke gegevens om deze aanvallen te voorkomen werd onderstreept. De richtlijn moest dan ook het gebruik van communicatiegegevens mogelijk maken, zij het binnen een kader van de bescherming van persoonsgegevens en privacy. Om die reden werden belangrijke vereisten naar de bewaringstermijn, de toegang tot deze gegevens, wijze van bewaring en gebruik vastgesteld.

6 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, Jur. L-105, 54–63. Hierna "dataretentierichtlijn".

7 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, PB L 281 van 23.11.1995, 31. Deze richtlijn werd vervangen door de Algemene Gegevensbeschermingsverordening (AGV). Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pub.* L-119, 1 - 18.

8 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),*PB* L 201 van 31.7.(2002): 37.

De dataretentierichtlijn voorzag in uniforme definities van communicatiegegevens (artikel 2) alsook duiding over welke gegevens de autoriteiten bewaringsregels mochten opleggen aan de operatoren van elektronische communicatienetwerken (artikel 3).[9] Dit omvat identificatiegegevens die het mogelijk maken om de verzender en ontvanger te identificeren, locatiegegevens die het mogelijk maken om de verzender en ontvanger te lokaliseren en verkeersgegevens die informatie gegeven over de communicatie zoals de duur, datum en tijdstip van de communicatie. Het bewaren van de inhoud van communicatie werd uitdrukkelijk uitgesloten, met inbegrip van de informatie die wordt geraadpleegd met behulp van een elektronisch communicatienetwerk (artikel 1).[10] Weliswaar moest deze richtlijn binnen de 2 jaar omgezet worden, het duurde tot 2013 en onder dreiging van Europese inbreukprocedures, dat de Belgische overheid deze richtlijn omzette in de dataretentiewet.[11] Hierbij werd de Wet Elektronische Communicatie[12] (hierna: WEC) aangepast zodat de telecombedrijven en digitale spelers verplicht werden om deze gegevens te bewaren voor een periode van 2 jaar. Het Wetboek van Strafvordering werd aangepast om het openbaar ministerie toe te laten bewaarde identificatiegegevens op te vragen en de onderzoeksrechter bewaarde locatie – en verkeersgegevens in het kader van strafonderzoeken. De Wet houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna: Wet inlichtingendiensten)[13] werd eveneens aangepast om toegang tot deze gegevens mogelijk te maken.

Vanuit mensenrechtelijke perspectief betekende de omzetting van de richtlijn door België een verbetering van de status quo omdat de eerdere wet reeds de bewaring van telefoniegegevens verplichtte, maar nu duidelijkere regels over de verwerking, bewaring en toegang tot de gegevens werden opgelegd. Dit was echter niet het geval voor gegevens die bewaard werden door de operatoren en dienstverleners van digitale communicatie, zeg maar alle communicatie die over het internet verloopt. Deze gegevens moesten immers voor de richtlijn niet bewaard worden. Daardoor werd de bescherming van persoonsgegevens en privacy beperkt ten voordele van de strijd tegen de criminaliteit en de bescherming van de openbare veiligheid.

Niet lang nadat België de richtlijn had omgezet, vernietigde het Hof van Justitie de dataretentierichtlijn in het *Digital Rights Ireland*- arrest[14] omdat deze in strijd was met de E-privacy richtlijn[15] alsook het recht op privacy en de bescherming van persoonsgegevens, zoals voorzien in de artikelen 7 en 8 van het EU Handvest voor

9 Over deze definities Jan-Jaap Oerlemans, Mireille Hagens en Sofie Royer, "Tijd voor een nieuwe bewaarplicht?", *Computerrecht,* vol. 59 (2021) 152 - 154; Robrecht De Keersmaecker en Catherine Van de Heyning, "De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga", *T.Strafr,* nr. 4 (2021): 171.

10 De inhoud van de communicatie maakt dan ook de kern van het recht op de bescherming van privacy uit waardoor hieraan niet geraakt kan worden. In die zin: Maja Brkan, "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning", *German Law Journal;* nr. 20 (2019): 871 – 874; Elif Mendos Kuskonmaz en Elspeth Guild, "Rights-Based Review of Border Surveillance", *The Charter and the Court of Justice of the European Union: Notable Cases from 2016-201*8 (Wolf Publishing: 2019): 96.

11 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 90decies van het Wetboek van Strafvordering, BS 23 augustus 2013, 56109. De wet kreeg verdere uitvoering via het 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. Hierover: Catherine Van de Heyning, "Data retention in Belgium", *European Constitutional Courts towards Data Retention Laws* (New York: Springer, 2021): 43 -74.

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

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

14 HvJ 8 april 2014, Zaak C-293/12 en 594, *Digitial Rights Ireland Ltd. en Kärtner Landesregierung,* ECLI:EU:C:2014:238.

15 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), Jur. L-201, 0037 – 0047.

de bescherming van fundamentele rechten.[16] Het Hof oordeelde dat het bijhouden van de verkeer – en locatiegegevens van iedereen voor de strijd tegen criminaliteit een disproportionele beperking van deze rechten uitmaakt en daardoor in strijd is met het Unierecht (r.o. 58 – 29).[17] Een dergelijke bewaring is enkel mogelijk als er objectieve redenen zijn voor die bewaring, bijvoorbeeld omdat deze persoon verdacht is of contact heeft met een persoon die verdacht wordt van een misdrijf. Een algemene, ongedifferentieerde bewaring van elektronische communicatiegegevens betekent per definitie dat de meerderheid van de bewaarde gegevens deze van personen zijn die geen uitstaan hebben met criminele of staatsgevaarlijke activiteiten. Daardoor mist er een verantwoording om de bescherming van de privacy en persoonsgegevens van deze personen te beperken door hun communicatie bij te houden. Het Hof benadrukte dat naast deze rechten, een algemene dataretentie ook de vrijemeningsuiting ondermijnt (r.o. 28). Als gegevens over elke communicatie worden bijgehouden, zullen personen meer opletten welke communicatie ze naar wie versturen en zich zelfcensuur opleggen. Een algemene dataretentie kan daarom een 'chilling effect'[18] hebben op de vrijemeningsuiting, en dit in het bijzonder voor opposanten van het overheidsbeleid, verdedigers van mensenrechten of minderheden.

In navolging van dit arrest vernietigden verschillende nationale grondwettelijke hoven de nationale regelgeving of beslisten hoogste gerechtshoven om deze wetgeving niet meer toe te passen. Ook het Grondwettelijk Hof vernietigde de Belgische dataretentiewet in lijn met de rechtspraak van het HvJ.[19] De Belgische wetgever reageerde in 2016 door een nieuwe dataretentiewetgeving in te voeren (dataretentiewet II).[20] Deze wet zocht een nieuw evenwicht waarbij enerzijds de algemene retentie van identificatie -, verkeer – en locatiegegevens werd behouden maar de toegang tot deze gegevens en het gebruik hiervan voor het bestrijden van misdaad en voor de nationale veiligheid werd beperkt. Ook deze wet en andere nationale regels over dataretentie werden aangevochten voor het Hof van Justitie. Al in 2018 oordeelde het Hof van Justitie in de arresten *Tele2/Watson*[21] dat de principes

16 In dit arrest en de andere dataretentie-arresten lag de nadruk grotendeels op de fundamentele rechten zoals vervat in het Handvest eerder dan de E-privacy richtlijn waardoor een loutere wijziging van deze richtlijn geen essentiële wijziging in de rechtspraak zal bewerkstelligen aangezien het Handvest primair recht is terwijl een richtlijn slechts secundair recht is. Hierover: Marcin Rojszcak, "The uncertain future of data retention laws in the EU: Is a legislative reset possible?", *Computer Law & Security Review,* vol. 41, 05572 (2021).

17 Een uitgebreide bespreking van dit arrest: Orla Lynskey, " The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland", *Common Market Law Review,* afl. 6 (2014): 1789–1811; Vainio en Miettinen, "Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States", 290–309; Andrew Roberts, "Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications", *The Modern Law Review,* vol. 78, nr. 3 (2015): 535 – 548.

18 Advocaat General Saugmandsgaard Øe verwees hierbij naar onderzoek van de VN Special Rapporteur voor de bevordering en bescherming van mensenrechten in de strijd tegen terrorisme (A/HRC/13/37) waaruit bleek dat 52 percent van bevraagde personen aangaf waarschijnlijk geen telecommunicatie te gebruiken voor bepaalde contacten, onder andere met psychotherapeuten, indien hun gegevens van communicatie bewaard werden. Opinie AG Saugmandsgaard Øe 19 juli 2016, gevoegde zaken C-203/15 en C-698/15, *Tele2 Sverige AB* / Watson, ECLI:EU:C:2016:572, voetnoot 84.

19 GwH 11 juni 2015, nr. 84/2015, *NC* 2015, afl. 6, 492-796. Hierover: F. Henrotte, "L' invalidation de la directive 2006/24 sur la conservation des données de communication électronique ou la chronique d'une mort annoncée", *JLMB* (2015): 956-957; Sarah Verstraelen, "De vernietiging van de Belgische datarententiewet met terugwerkende kracht: de bescherming van het privéleven primeert", *NC* (2015): 492-496; Michele Panzavolta, Sofie Royer and Helena Severijns, "Algemene dataretentie: ten minste houdbaar tot …?", *T.Strafr.* 2018, afl. 1, 7 – 8 en C. Conings, "Dataretentie en privacy", *NJW* afl. 333 (2015): 911 – 912.

20 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, 44717.Hierover Panzavolta, Royer and Severijns, "Algemene dataretentie: ten minste houdbaar tot …?", 7; Charlotte Conings, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, Antwerpen (2017): 181 – 202; Charlotte Conings en Kristel De Schepper, "Dataretentie: tweede keer, goede keer", *Juristenkrant* (2016): 12; Philip Daeninck, *Telefonieonderzoek in het strafrecht - Het triumviraat van de artikelen 46bis, 88bis en 90ter Sv.*, (Brugge: Die Keure, 2021): 7 – 11; Van de Heyning, "Data retention in Belgium", 43 -74; Bart De Smet, "Nieuwe regels voor dataretentie van telecomoperatoren: een obstakel voor de waarheidsvinding?", *RW,* vol. 11 (2016): 402.

21 HVJ 21 december 2016, zaak C-203/15 en C-698/15, *Tel2 Sverige AB t. Post - och telestryrelsen en Secretary of state for the Home Department t. Tom Watson e.a.*, ECLI:EU:C:2016:970 (hierna: Tele2/Watson).

weerhouden in het *Digital Rights Ireland* – arrest ook gelden voor nationale dataretentiewetgeving. Ook op nationaal niveau is de algemene retentie van communicatiegegevens slechts mogelijk in zover het voorzien is bij wet, een objectieve doelstelling dient en proportioneel is. Het Hof maakte daarbij een onderscheid tussen identificatiegegevens, die minder privacygevoelig zijn, en locatie – en verkeersgegevens, die veel informatie over het privéleven van de persoon weergeven.[22] Waar een algemene bewaarplicht voor identificatiegegevens voor de strijd tegen ernstige criminaliteit mogelijk is, oordeelt het HvJ dat een algemene bewaring van locatie – en verkeersgegevens voor de strijd tegen misdaad een disproportionele beperking van het recht op privacy en persoonsgegevens uitmaakt (*Tele2/Watson* r.o. 107). Toen het Grondwettelijk Hof de vraag werd gesteld om de nationale dataretentiewet 2016 in overeenstemming was met het recht op privacy en persoonsgegevens zoals vervat in het Unierecht, was de verwachting dat het Hof zou oordelen dat deze wet ontkennend zou beoordelen.[23] De wet bleef immers vasthouden aan een algemene retentie van verkeer – en locatiegegevens, wat het HvJ duidelijk in strijd met het Unierecht bevond. Toch stuurde het Grondwettelijk Hof enkele prejudiciële vragen naar het HvJ met inbegrip van de vraag of een dergelijke algemene retentie wel was toegelaten indien dit werd vergezeld met een beperkte toegang tot de gegevens.[24] Ook Franse, Ierse, Britse, en Estse hoogste gerechtshoven stuurden prejudiciële vragen naar het Hof van Justitie voor verdere verduidelijking van haar dataretentierechtspraak.

Zicht op dataretentie: wie en hoeveel

De Europese rechtspraak, in het bijzonder de arresten *Tele2/Watson*, werden door verschillende lidstaten met ontsteltenis onthaalt. Waar hun eigen regelgeving duidelijk in strijd was met de Europese rechtspraak omdat het voorzag in een algemene dataretentie waren er slechts enkelingen die hun regelgeving hierop aanpasten. De lidstaten protesteerden dat deze gegevens noodzakelijk waren voor de strijd tegen criminaliteit en voor de nationale veiligheid. Ze betoogden dat zonder deze gegevens de veiligheidsdiensten, politie en justitie nog bijzonder moeilijk onderzoek zouden kunnen voeren nu het gros van communicatie naar het digitale was verschoven. Dit werd in het bijzonder als problematisch aangevoeld voor misdrijven en aanvallen die volledige online plaatsvinden, zoals hacking, ransomware of kindermisbruikmateriaal.

Dat deze gegevens veelvuldig en steeds meer gebruikt worden door zowel justitie als de inlichtingendiensten blijkt uit de cijfers van het Belgisch Instituut voor Postdiensten en Telecommunicatie.[25] Uit de gepubliceerde statistieken blijkt dat operatoren van elektronische-communicatiediensten steeds vaker gegevens verstrekten. Het aantal gegevens dat justitie verkreeg in het kader van strafonderzoeken verviervoudigde op een periode van 4 jaar tussen 2014 en 2018. Daarbij waren

22 Het Hof bepaalt dat: "Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren". *Tele2/Watson,* vn 19, § 99

23 Zie o.a. Panzavolta, Royer en Severijns, "Algemene dataretentie: ten minste houdbaar tot ...?", 7; Sofie Royer en Charlotte Conings, "Ook hervormde dataretentiewet staat onder druk", *Juristenkrant*, iss 134 (2017): 1; Catherine Van de Heyning, "Het gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek in gevaar?", *RABG,* iss 7 (2017): 533 – 538; Catherine Forget, "L'obligation de conservation des "métadonnées", la fin d'une longue saga juridique?", *JT* (2017).

24 GwH 19 juli 2018, nr. 96/2018 (Ordre des barreaux francophones et germanophone, vzw Académie Fiscale en Jean Pierre Riquet, e.a.). Zie Sofie Royer, "Dataretentie: Grondwettelijk Hof stelt prejudiciële vraag aan Hof van Justitie", *Computerrecht*, nr. 5 (2018): 247; Catherine Van de Heyning, "Overzicht van rechtspraak – Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog", *T.Strafr.*, afl. 1 (2018): 38 – 47.

25 BIPT, Statistische inlichtingen inzake dataretentie, te raadplegen: https://www.bipt.be.

deze bevragingen goed voor het grote merendeel van de verzoeken. Ook het aantal verzoeken door de inlichtingendiensten steeg spectaculair tussen 2014 en 2018, maar vertegenwoordigt slechts een bescheiden aantal verzoeken, in het bijzonder in vergelijking met de bevragingen door justitie. Vanaf 2019 werden geen cijfers meer gepubliceerd.

Opgevraagde gegevens	Door justitie		Door inlichtingendiensten	
	aantal	% t.a.v. totaal	Aantal	% t.a.v. totaal
2014	225 618	95,6%	1721	0,7%
2015	219 386	94,2%	2739	1,8%
2016	230 476	95,7%	3 766	1,6%
2017	821 617	96,9%	19 552	2,7%
2018	893 281	96,5%	23 939	2,6%

De gegevens van dienstverleners van elektronische communicatie op basis van hun eigen transparantierapporten geven aan dat deze trend zich verderzette in de laatste jaren. Waar de Facebook-groep in 2013 slechts 305 verzoeken kreeg van Belgische autoriteiten met betrekking tot 365, ontving het in 2020 wel 1697 verzoeken voor data met betrekking tot 12 933 accounts.[26] Google noteerde 365 verzoeken voor 495 accounts in 2013 ten opzichte van 1 261 verzoeken in 2020 voor 2404 accounts.[27] Deze cijfers geven net zoals de BIPT-cijfers een spectaculaire stijging aan in het aantal verzoeken. Daarmee volgt België een wereldwijde evolutie waarbij vervolgende instanties steeds vaker communicatiegegevens opvragen in het kader van lopende onderzoeken.[28] Er zijn echter ook cijfers die dan weer eerder stabiel blijven. Microsoft werd 878 maal bevraagd in 2013 voor 1304 accounts, terwijl het bedrijf in de eerste 6 maanden van 2021 een 446 maal bevraagd werd voor 604 accounts.[29]

Wie al deze cijfers naast elkaar legt, komt tot de conclusie dat verstrekkers van elektronische communicatienetwerken steeds meer bevraagd worden en dit voor gegevens van steeds meer gebruikers. Bovendien gebeurt het gros van de bevragingen door justitie. Dit betekent dat deze gegevens vooral bevraagd worden in het kader van strafonderzoeken. Dit betekent nog niet automatisch dat deze gegevens ook leidden tot vervolgingen of identificatie van verdachten, maar minstens geeft het aan dat het openbaar ministerie dan wel onderzoeksrechter veelvuldig meenden deze gegevens te moeten bevragen in het kader van het strafonderzoek. De andere diensten die toegang nemen tot deze gegevens, zijnde de inlichtingendiensten, Ombudsdiensten en hulpverleners, vertegenwoordigen slechts een fractie van het totaal aantal bevragingen. Evenmin kan uit deze cijfers eenvoudigweg uitgemaakt worden wat het belang van de bevragingen waren, bijvoorbeeld kunnen de door de inlichtingendiensten bevraagde gegevens veel gerichter geëxploiteerd worden dan het grote aantal van gegevens door de justitiële autoriteiten.

26 Facebook transparency report: https://transparency.fb.com/data/government-data-requests/country/BE/.
27 Google transparency report: https://transparencyreport.google.com/.
28 Catherine Jasserand, "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?", *Computer Law & Security Review* vol. 34, nr. 1 (2018): 154.
29 Law Enforcement Requests Report: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

Een verdere exploitatie van de cijfers alsook het gebruik van de gegevens door zowel strafrechtelijke autoriteiten als inlichtingendiensten zou nuttig zijn voor de rol van elektronische communicatiegegevens in de strijd tegen misdaad en voor de bescherming van de nationale veiligheid, o.a. voor vragen naar de reden waarom deze gegevens gebruikt werden en welke rol ze uiteindelijk speelden in het verdere onderzoek. Wat in elk geval vaststaat, is de grote stijging in bevraagde gegevens, in het bijzonder door justitie, waaruit blijkt dat voor strafonderzoeken deze gegevens veelvuldig gebruikt worden. Een beperking in dataretentie en dus 'bevraagbare' gegevens zal dan ook in het bijzonder op de wijze waarop strafonderzoeken gevoerd worden een grote impact hebben.

Een Europees evenwicht in de Europese rechtspraak

De basisprincipes in steen gebeiteld

In navolging van de *Tele2/Watson* – arresten werd het Hof van Justitie intussen reeds verschillende malen opnieuw bevraagd over de bewaring van telecommunicatiegegevens in de strijd tegen criminaliteit. In de arresten *Ministerio Fiscal*[30] van 2016, *La Quadrature du Net* (*LQDN*)[31] en *Privacy International*[32] van 2020, *Prokuratuur*[33] van 2021 en *Commissioner of the Garda Síochána*[34] *(An Garda Síochána)* van 2022, kon het Hof van Justitie haar rechtspraak over de toelaatbaarheid van de bewaring van elektronische communicatiegegevens alsook het gebruik en de toegang daartoe verder verduidelijken.[35]

Algemene retentie van locatie – en verkeersgegevens voor de strijd tegen misdaad uitgesloten

Het Hof van Justitie bevestigde in deze arresten de eerdere lijn dat een algemene retentie van locatie – en verkeersgegevens voor de strijd tegen criminaliteit het recht op privacy en de bescherming van persoonsgegevens schendt en daardoor niet is toegestaan. De bewaring van locatie – en verkeersgegevens zijn volgens het HvJ een bijzonder ernstige beperking van het privéleven en bescherming van persoonsgegevens omdat ze een intiem beeld kunnen geven over het leven van diegene wiens gegevens worden verzameld. Dit is in het bijzonder het geval wanneer deze gegevens details onthullen over de seksuele oriëntatie, religie, politieke overtuiging of nog andere persoonlijke criteria.

Om dergelijke gegevens te bewaren moet er een grondige verantwoording zijn voor de beperking van deze fundamentele rechten. Het Hof van Justitie erkent dat de bescherming van de openbare veiligheid en de strijd tegen de criminaliteit ernstige overwegingen zijn, maar niet kunnen verantwoorden dat de gegevens van iedereen worden bijgehouden en dus ook van personen die geenszins gelinkt zijn met criminaliteit.

30 HvJ 2 oktober 2018, Zaak C-207/16, *Ministerio Fiscal,* ECLI:EU:C:2018:788.
31 HvJ 6 oktober 2020, Gevoegde zaken C-511/18, C-512 en C-520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791.
32 HvJ 6 oktober 2020, Zaak C-623-17, *Privacy International,* ECLI:EU:C:2020:790.
33 HvJ 2 maart 2021, Zaak C-7-46/18, *Prokuratuur*, ECLI:EU:C:2021:152.
34 HvJ 5 april 2022, Zaak C-140/20, *Commissioner of the Garda Síochána e.a,* ECLI:EU:C:2022:258.
35 Over deze arresten zie Oerlemans, Hagens en Royer, "Tijd voor een nieuwe bewaarplicht?", 155 – 156; De Keersmaecker en Van de Heyning, "De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga", 171.

Gerichte retentie van locatie – en verkeersgegevens in de strijd tegen misdaad mogelijk

Gerichte bewaring van locatie – en verkeersgegevens is wel mogelijk indien er een voldoende objectieve verantwoording is voor deze bewaring en deze niet-discriminatoir is. Uit de rechtspraak bleek dat de gerichte retentie van locatie – en verkeersgegevens als een proportionele beperking van fundamentele rechten wordt beschouwd indien deze beperkt zijn tot bepaalde categorieën van personen, strategische plaatsen en bepaalde geografische zones (*LQDN* r.o. 150). Advocaat-Generaal Campos Sanchez-Bordona noemde deze gerichte bewaring van locatie – en verkeersgegevens zelfs "de hoeksteen van de redenering in de arresten van het Hof ter zake".[36]

Voor wat de *categorieën van personen* betreft omvat dit minstens personen die rechtstreeks (verdachten) of onrechtstreeks (nauwe contacten van de verdachten) betrokken zijn bij een strafonderzoek naar bepaalde feiten. Dit kan ook gaan om personen die door de inlichtingendiensten op basis van objectieve gegevens worden opgevolgd, bijvoorbeeld vanwege gegevens die wijzen op radicalisering.

Voor wat de *strategische zones* betreft, verwees het HvJ naar vliegvelden, stations, zeehavens of tolzones als dergelijke strategische plaatsen, maar eveneens andere plaats die een kritische of essentiële rol vervullen dan wel waar een bijzonder veiligheidsrisico is vanwege de aard van de activiteit die daar plaatsvindt, kunnen hieronder vallen, zoals nucleaire sites of militaire domeinen. Op die plaatsen kunnen de autoriteiten de locatie – en verkeersgegevens doen bewaren van iedereen die op een gegeven moment op een van die plaatsen een elektronisch communicatiemiddel gebruikt (*An Garda Síochána* r.o. 81).

Tot slot laat het HvJ eveneens toe dat er een algemene retentie is *binnen bepaalde zones* waar veel zware criminaliteit plaatsvindt, op plaatsen waar er een verhoogd risico is op zware strafbare feiten, of plekken en faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht. Deze zones kunnen bepaald worden op basis van concrete aanwijzingen dat er in die zones zware misdaden worden voorbereid of gepleegd (*An Garda Síochána* r.o. 80). Het gaat dus zowel over zones waar een groot aantal zware misdaden werd gepleegd als waar er op basis van objectieve gegevens een verhoogd risico is, bijvoorbeeld naar aanleiding van een aangekondigde betoging waar rellen worden verwacht. Het Hof licht toe dat het afbakenen van deze zones op basis van een criminaliteitscijfers, waarbij worden gekeken naar het gemiddelde van zware criminaliteit, niet discriminerend is maar berust op objectieve gronden (ibid.). Bewaringsmaatregelen voor geografische zones kunnen per definitie niet statisch zijn. Het HvJ benadrukt dat gerichte bewaringsmaatregelen op geviseerde geografische zones moeten worden aangepast indien:

> "de omstandigheden die de selectie ervan rechtvaardigden, wijzigen, waardoor met name kan worden ingespeeld op veranderingen in de strijd tegen zware criminaliteit"(*An Garda Síochána* r.o. 82) .

Dit volgt logisch uit de eerdere rechtspraak van het Hof waarin werd geoordeeld dat maatregelen van gerichte gegevensbewaring slechts zo lang mogen duren als strikt noodzakelijk in het licht van het beoogde doe van de retentie en van de omstandigheden die de bewaring verantwoorden (*LQDN* r.o. 151). Verlengingen zijn dus mogelijk, maar slechts op voorwaarde van een controle of de redenen voor de initiële maatregel nog steeds aanwezig zijn.

36 Opinie Advocaat-Generaal Campos Sanchez-Bordona 18 november 2021, Zaak C-140/20, *The Commissioner of the Garda Síochána*, ECLI:EU:C:2021:942, r.o. 43.

Algemene retentie van identificatiegegevens wel mogelijk

In tegenstelling tot locatie – en verkeersgegevens, oordeelde het HvJ dat de bewaring van identificatiegegevens een beperkte inbreuk vormt op het privéleven en de bescherming van persoonsgegevens. Deze gegevens geven enkel informatie over de identiteit van personen en toestellen, maar niets over de communicatie zelf. Een algemene retentie van deze gegevens is wel mogelijk voor het bestrijden van ernstige criminaliteit. Het Hof van Justitie verduidelijkte in het arrest *Ministerio Fiscal* dat het aan de lidstaten toekomt om te bepalen wat een 'ernstig misdrijf' uitmaakt zolang dit berust op een objectieve verantwoording rekening houdende met de ernst van de beperking op de fundamentele rechten en de ernst van het misdrijf (r.o 58 - 62). Op deze basis besloot het Grondwettelijk Hof reeds dat de wettelijke verplichting voor de registratie en bewaring van de identiteit van kopers en gebruikers van SIM-kaarten in lijn is met de rechtspraak van het Hof van Justitie.[37] In het arrest *La Quadrature du Net* bevestigde het HvJ dat informatie over de burgerlijke identiteit van een gebruiker identificatiegegevens uitmaken die op algemene wijze bewaard mogen worden (*LQDN* r.o. 157).

Het Hof van Justitie verduidelijkte bovendien dat IP-adressen ook identificatiegegevens uitmaken en dus op algemene wijze bewaard kunnen worden (*LQDN* r.o. 154). Deze conclusie was niet evident. IP-adressen zijn een reeks cijfers en letters die eigen zijn aan apparaten die verbonden zijn met een computernetwerk. Op basis van IP-adressen kan dus nagegaan worden vanuit welke apparaat er een connectie met het computernetwerk werd gemaakt en wie, minstens welk toestel, er achter mogelijke feiten schuilgaat.[38] Op die manier kan een persoon echter ook gelokaliseerd worden. Immers, op basis van deze adressen kan een operator of dienstverlener van een elektronische communicatiedienst registreren waar het toestel zich bevindt en bijvoorbeeld voorkomen dat een Europese consument goedkoper bepaalde online diensten probeert aan te schaffen via een platform van hetzelfde bedrijf in een ander land. Bovendien kunnen IP-adressen informatie geven over de *browsing*-geschiedenis, namelijk over welke webpagina's en platformen werden bezocht. Deze informatie kan een intiem beeld schetsen over het privéleven van een persoon. Het HvJ besloot dat IP-gegevens cruciaal zijn voor strafrechtelijke onderzoeken en zonder de retentie van deze gegevens het onderzoek naar als de vervolging en bestraffing van misdrijven, in het bijzonder cybercrime, onmogelijk is (*LQDN* r.o. 154). Om die reden oordeelde het HvJ dat IP-adressen eveneens op een algemene wijze bewaard mogen worden om ernstige criminaliteit te bestrijden, zij het enkel IP-adressen die zijn toegewezen aan de bron van een verbinding en mits omstandige procedurele waarborgen (*LQDN* r.o. 155).

Uitzonderingen voor de bescherming van de nationale veiligheid

In tegenstelling tot de strijd tegen misdaad en de bescherming van de openbare orde, meende het HvJ dat een algemene bewaarplicht van locatie – en verkeersgegevens wel verantwoord is voor de bescherming van de nationale veiligheid. Het HvJ benadrukte daarbij het belang van de bewaring van deze gegevens in de strijd tegen terrorisme (*LQN* r.o. 139). Deze bewaring is mogelijk omdat de bescherming van de nationale veiligheid volgens het Hof een voldoende ernstig belang uitmaakt waardoor de beperking van de artikelen 7 – 8 Handvest in het licht hiervan proportioneel is. Deze algemene bewaring is echter alleen mogelijk als er sprake is

37 GwH 18 november 2021, nr. 158/2021.

38 Het Hof van Justitie erkent in het arrest *LQDN* ook de duale aard van IP-adressen in r.o. 152 – 153. Uitgebreid over IP-adressen in het kader van dataretentie De Keersmaecker en Van de Heyning, "De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga", 171.

van een imminente dreiging voor de nationale veiligheid. De autoriteiten zullen dus moeten aantonen dat er sprake is van een ernstige, werkelijke en actuele dan wel voorzienbare dreiging voor de nationale veiligheid (*LQN*, r.o. 168 en *Privacy International*, r.o.). Ook het Europees Hof voor de Rechten van de Mens oordeelde al in die zin, namelijk dat een algemene bewaring van locatie – en verkeersgegevens geen schending van het recht op privacy vervat in artikel 8 EVRM is indien er een werkelijke en actuele of voorzienbare bedreiging voor de nationale veiligheid is.[39]

Gezien dergelijke algemene retentie enkel mogelijk is bij een imminente en ernstige dreiging en daardoor tijdelijk, moeten de autoriteiten deze dreiging periodiek evalueren. Indien de dreiging dus vermindert, is een algemene retentie niet langer verantwoord. De nationale autoriteiten moeten daarom de operatoren en dienstverleners van elektronische communicatienetwerken een bewaringsbevel overmaken waarin de periode van bewaring wordt voorzien. Een dergelijk bevel kan verlengd worden, mits evaluatie van de al dan niet blijvende dreiging voor de nationale veiligheid. Een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit moet deze bewaringsbevelen kunnen toetsen aan zowel de wettelijke vereisten van deze bevelen als aan het vereiste van een imminente en ernstige dreiging voor de nationale veiligheid (*LQN* r.o. 139). De overheid kan zich dus niet verschuilen achter een geheimhouding voor de vereisten van de nationale veiligheid om deze instanties toegang te ontzeggen tot de bewaringbevelen. De beoordeling van het bewaringsbevel moet bovendien bindend zijn.

Op deze uitzondering voor de nationale veiligheid kwam veel kritiek. Ten eerste benadrukten privacy-experten dat het HvJ hiermee terugkomt op haar eerdere rechtspraak waar het de algemene retentie van locatie – en verkeersgegevens op algemene wijze uitsloot en geen uitzondering voorzag voor de nationale veiligheid. Volgens Sajfert antwoordt het HvJ daarmee op de kritiek van de lidstaten dat het gebrek aan deze data de nationale veiligheid ernstig zou ondermijnen, in het bijzonder in de strijd tegen terrorisme.[40] Ten tweede was er kritiek van de lidstaten en vervolgende autoriteiten op de keuze van het HvJ om een algemene retentie van locatie – en verkeersgegevens wél toe te laten voor de bescherming van de nationale veiligheid en niet voor de strijd tegen ernstige criminaliteit en een ernstige verstoring van de openbare orde. Concreet zou dit betekenen dat deze gegevens wel bewaard mogen worden zodat de inlichtingendiensten een terroristische aanslag kunnen voorkomen, maar niet voor het strafonderzoek naar de daders indien er zo'n aanval heeft plaatsgevonden. De Europese commissie beargumenteerde voor het Hof van Justitie dat zeer ernstige criminaliteit een bedreiging voor de nationale veiligheid betekent en om die reden ermee gelijkgesteld moet worden.[41] Het Belgische grondwettelijke hof had in haar prejudiciële vraag aan het Hof van Justitie benadrukt dat op de lidstaten ook positieve verplichtingen rusten zoals de bescherming van het recht op leven.[42] Een beperkte bewaring van locatie – en verkeersgegevens zou het onderzoek naar misdrijven die een inbreuk op dat recht uitmaken bemoeilijken. In het arrest *La Quadrature du Net* erkent het Hof van Justitie dat deze positieve verplichtingen lidstaten ertoe verplichten om materiële en procedure

39 EHRM 25 mei 2021, *Big Brother Watch e.a. t. Verenigd Koninkrijk* en EHRM 25 mei 2021, *Centrum för Rättvisa t. Zweden*. Hierover zie Juraj Sajfert, "The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?", *European Law Blog* 8 juni 2021, te raadplegen: https://europeanlawblog.eu, Marko Milanovic, "The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa", *EJIL Talk!* 26 mei 2021, te raadplegen: www.ejiltalk.org; Mark Klamberg, "Big Brother's little, more dangerous brother", *Verbassungsblog* 1 juni 2021, te raadplegen: https://verfassungsblog.de/raettvisa.

40 Juraj Sajfert, "Bulk data interception / retention judgments of the CJEU - A victory and a defeat for privacy", European law blog 26 oktober 2020, te raadplegen: https://europeanlawblog.eu.

41 Opinie AG Campos Sanchez-Bordona 18 november 2021, Zaak C-140/20, The Commissioner of the Garda Síochána, ECLI:EU:C:2021:942, r.o. 51. De Advocaat-Generaal merkt op dat deze visie gesteund werd door "belangrijk deel van de ter terechtzitting vertegenwoordigde regeringen". Opinie AG Campos Sanchez-Bordona, vn 31.

42 GwH 19 juli 2018, nr. 96/2018.

bepalingen als praktische maatregelen te nemen om criminaliteit tegen personen, zoals kindermisbruik, doeltreffend te onderzoeken en vervolgen (LQDN r.o. 128). Desondanks meent het HvJ dat deze positieve verplichtingen geen dusdanige ingrijpende beperking van het recht op privacy en bescherming persoonsgegevens kunnen verantwoorden waarbij de verkeers- en locatiegegevens kunnen worden bewaard zonder dat de gegevens van de betrokken personen verband houden met de bestrijding van misdrijven (LQDN r.o. 145). Deze positieve verplichtingen voor de bescherming van de nationale veiligheid kan daarentegen wel een algemene retentie verantwoorden in zover er een imminent en ernstig gevaar dreigt, omdat een dergelijke dreiging een impact heeft op elke burger.

In *Commissioner of the Garda Síochána* bevraagt het Ierse Surpeme Court het HvJ opnieuw over dit onderscheid. De Supreme Court vroeg of het wel verantwoord was dat locatie – en verkeersgegevens niet mogen bewaard worden voor de strijd tegen criminaliteit, zelfs niet voor bijzonder ernstige misdrijven zoals doodslag, terwijl operatoren en dienstverleners deze wel mogen bewaren voor hun eigen commerciële doeleinden en ook voor de nationale veiligheid onder bepaalde voorwaarden. Het HvJ antwoorde reeds in het arrest *Privacy International* dat de nationale veiligheid een bijzonder ernstig belang is dat zelfs de bestrijding van ernstige criminaliteit overstijgt en om die reden de ernstige beperking kan verantwoorden die de algemene retentie van locatie – en verkeersgegevens betekent voor het recht op privacy en de bescherming van persoonsgegevens (r.o. 75).

Het HvJ geeft in het arrest *An Garda Síochána* bijkomend drie onderliggende redenen waarom de strijd tegen ernstige criminaliteit verschilt van de bescherming van de nationale veiligheid. Ten eerste benadrukt het HvJ dat de bescherming van de nationale veiligheid de exclusieve bevoegdheid is van de lidstaten *(An Garda Síochána* r.o. 57). Ten tweede heeft de bescherming van de nationale veiligheid een impact op "de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren" (*An Garda Síochána* r.o. 61). Een aanval op de nationale veiligheid betekent een rechtstreekse bedreiging voor de samenleving, de bevolking en de staat. Ten derde wijst het HvJ erop dat deze algemene retentie voor de nationale veiligheid steeds tijdelijk is omdat deze enkel wordt ingesteld in het geval van een ernstige, reële en actuele dreiging. Hierin verschilt de bescherming van de nationale veiligheid volgens het Hof van de strijd tegen criminaliteit, omdat in een maatschappij er een permanent risico is op bedreigingen voor de openbare veiligheid en op criminaliteit (*An Garda Síochána* r.o. 62). Daardoor, besluit het Hof, verschilt de dreiging die uitgaat van aanvallen op de nationale veiligheid, zoals door terroristen, van deze meer permanente dreiging van criminaliteit en aanvallen op de openbare orde. Anders gezegd, de strijd tegen criminaliteit, ook ernstige criminaliteit, is onvoldoende uitzonderlijk en periodiek om een dergelijke algemene beperking voor de hele bevolking op het recht op privacy en de bescherming van persoonsgegevens te verantwoorden.

De lijn tussen bewaring, toegang en gebruik uitgeklaard

Naast de vraag over welke data bewaard mogen worden, ging het HvJ in haar rechtspraak ook in op de toegang tot deze gegevens. Het Hof verwierp reeds de redenering van de Belgische wetgever dat de bewaring en toegang samen bekeken moesten worden in die zin dat een beperkte toegang tot de gegevens door bevoegde autoriteiten een algemene bewaarplicht kon rechtvaardigen. Deze moeten volgens het Hof apart beoordeeld worden op de verenigbaarheid met de bescherming van privacy en persoonsgegevens (*An Garda Síochána* r.o. 47). Dit is een logische

beoordeling vanuit de bredere filosofie achter de bescherming van persoonsgegevens waarbij elke verwerking van deze gegevens conform de bescherming van fundamentele rechten moet zijn, en dus ook zowel de bewaring door de operatoren en dienstverleners als de toegang en het gebruik van deze gegevens door bevoegde autoriteiten zoals vervolgende instanties.

Het Hof oordeelde in de eerste plaats dat er enkel toegang kon genomen worden tot deze gegevens voor onderzoek naar ernstige criminaliteit, waarbij het Hof een grote beoordelingsmarge voor de lidstaten laat naar wat een 'ernstig misdrijf' dan wel uitmaakt. De nationale rechter moet hierbij de ernst van de beperking aan de bescherming van de privacy en persoonsgegevens afwegen ten opzicht van de ernst van de strafbare feiten (*Ministerio Fiscal* r.o. 56 - 62). In de tweede plaats ging het Hof ook in op de vraag tot welke bewaarde gegevens de vervolgende partijen toegang kunnen nemen. Concreet, mag een autoriteit voor een doelstelling, bijvoorbeeld het oplossen van een strafzaak, enkel toegang nemen tot de gegevens die voor deze doelstelling werden bewaarde, namelijk bewaard voor de strijd tegen ernstige criminaliteit, of ook deze bewaard voor andere doelstellingen, bijvoorbeeld voor de bescherming van de nationale veiligheid? In het arrest *La Quadrature du Net* antwoordde het HvJ dat autoriteiten voor de bescherming van de nationale veiligheid ook toegang mogen nemen tot gegevens die werden bewaard op basis van gerichte bewaarmaatregelen in de strijd tegen ernstige criminaliteit (*LQDN* r.o. 166). Bovendien mogen de bevoegde autoriteiten ook toegang nemen tot gegevens die rechtmatig bewaard werden door de operatoren en dienstverleners van elektronische communicatienetwerken op andere gronden, bijvoorbeeld facturatie of het verzekeren van de dienstverlening, zij het enkel voor de strijd tegen ernstige criminaliteit, een ernstige verstoring van de openbare orde of de bescherming van de nationale veiligheid (*LQDN* r.o. 167).

De vraag bleef echter of nationale autoriteiten ook toegang mogen nemen tot locatie – en verkeersgegevens die op algemene wijze bewaard werden voor de bescherming van de nationale veiligheid voor het oplossen van ernstige strafbare feiten. Het HvJ antwoordde hierop ontkennend in *Commissioner of the Garda Síochána*. Het Hof verdedigt deze beslissing door erop te wijzen dat als autoriteiten voor de strijd tegen ernstige criminaliteit ook toegang zouden kunnen krijgen tot algemeen bewaarde gegevens voor de bescherming van de nationale veiligheid dit de nuttige werking van het principiële onderscheid tussen de retentie voor de strijd tegen ernstige criminaliteit en voor de bescherming van de nationale veiligheid zou ondermijnen (*An Garda Síochána* r.o. 100). 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, wat zich visueel vertaald in volgend overzicht:

Communicatiegegevens	Bewaard voor commerciële reden	Bewaard voor strijd tegen ernstige criminaliteit	Bewaard voor bescherming nationale veiligheid
Toegang voor commerciële redenen	X	/	/
Toegang voor strijd tegen ernstige criminaliteit	X	X	/
Toegang voor bescherming van de nationale veiligheid	X	X	X

In de derde plaats beantwoorde het HvJ de vraag wie toegang mag nemen tot de bewaarde gegevens. Het Hof bevestigde verschillende keren dat de vraag wie toegang kon nemen mede afhankelijk was van het type van bewaarde gegevens, gezien toegang tot locatie – en verkeersgegevens een ernstigere beperking van het recht op privacy en de bescherming van persoonsgegevens uitmaakt dan bijvoorbeeld toegang tot identificatiegegevens. Het openbaar ministerie kan daardoor wel toegang nemen tot identificatiegegevens, maar niet rechtstreeks tot locatie – en verkeersgegevens (*Prokuratuur* r.o. 57). Tot deze gegevens kan er enkel toegang worden genomen na een toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteiten. Deze autoriteiten moeten hun beslissing over toegang tot locatie – en verkeersgegevens ook motiveren (*Prokuratuur* r.o. 51 - 52). 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.

Om die reden oordeelde het HvJ 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 (*Prokuratuur* r.o. 55 – 57). 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 t.a.v. 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 (LQDN 189). Dit geldt ook voor politie, waarbij een a posteriori toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit onvoldoende is (*An Garda Síochána* r.o. 111 – 112). Er was enige tijd discussie of deze rechtspraak verhinderde dat de onderzoeksrechter locatie – en verkeersgegevens kon opvragen.

Er werd betoogd dat conform de Luxemburgse rechtspraak de onderzoeksrechter niet over de vereiste onafhankelijkheid beschikt omdat hij het gerechtelijk onderzoek leidt en daardoor een belang zou hebben bij een brede dataretentie.[43] Hier kon tegenin gebracht worden dat een onderzoeksrechter geen enkele rol speelt in de verdere vervolging van een eventuele inverdenkinggestelde en in dat opzicht niet betrokken was bij de strafvordering.[44] Het arrest *An Garda Síochána* neemt alle twijfel weg doordat het duidelijk maakt dat de vereiste van onafhankelijk zoals het deze definieerde in *Prokuratuur* enkel van tel is voor bestuurlijke administraties die oordelen over de toegang tot locatie – en verkeersgegevens (*An Garda Síochána* r.o. 108). Voor rechterlijke instanties gelden de vereisten van onafhankelijkheid en onpartijdigheid van de rechterlijke macht zoals uitgewerkt door het Europees Hof voor de Rechten van de Mens op basis van artikel 6 EVRM. Vanuit deze rechtspraak voldoet de onderzoeksrechter binnen het Belgische recht aan deze vereisten.

43 Sofie Royer en Sem Careel, "Access denied – CJEU reaffirms la Quadrature du Net and clarifies requirements for access to retained data", *Citip Blog* 23 maart 2021, te raadplegen: www.law.kuleuven.be/citip/blog.

44 De Keersmaecker en Van de Heyning, "De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga", 171.

De Belgische impact van de Europese dataretentie regels

Vernietiging van de Belgische regelgeving en gevolgen voor lopende zaken

In navolging van het arrest van het Hof van Justitie vernietigde het Grondwettelijk Hof de 2016 dataretentiewet.[45] Er werd voorgehouden dat het Grondwettelijk Hof ook kon kiezen om artikel 126 van de wet elektronische communicatie slechts te vernietigen in zover er werd voorzien in een algemene retentie van locatie – en verkeersgegevens. Het Grondwettelijk Hof besloot echter dat dit onmogelijk was gezien deze bepaling op dat vlak geen onderscheid maakte en slechts voorzag in een algemene retentie van identificatie - , locatie – en verkeersgegevens. Het komt de wetgever toe om een gedifferentieerd regime bij wet in te voeren dat een onderscheid tussen de verschillende dataregimes voorziet. Het Hof vernietigde in dezelfde lijn de bepaling 88bis van het Wetboek van Strafvordering dat de onderzoeksrechter toegang geeft tot deze algemeen bewaarde gegevens aangezien deze toegang slechts mogelijk is tot gericht bewaarde gegevens op basis van een bewaringsbevel, waarin de wet elektronische communicatie noch het wetboek van strafvordering voorzagen.

Er werd gepleit voor overgangsbepaling zodat de wetgever een nieuwe regeling kon voorzien. Het Grondwettelijk Hof verwees op dit vlak naar de rechtspraak van het Hof van Justitie dat benadrukte dat het niet aan de nationale rechtscolleges toekwam om de werking in de tijd van haar arresten te beoordelen.[46] Het Hof van Justitie besliste dat er geen tijdelijke werking werd toegekend aan haar arrest *La Quadrature du Net* (*LQDN* r.o. 213 – 220). Deze beslissing was zonder twijfel beïnvloed door de vaststelling dat het Hof reeds in 2018 met de arresten *Tele2/Watson* de principes had uitgeklaard, maar de lidstaten talmden om hier gevolg aan te geven. Op het moment van publicatie van het arrest van het Grondwettelijk Hof werd de vernietiging van de wet elektronische communicatie voor wat de verplichte bewaring van communicatiegegevens betreft en artikel 88bis Wetboek van Strafvordering dan ook definitief. Hierdoor herleefde de oude bepaling artikel 126 WEC herleven waar echter geen algemene retentie van telecommunicatiegegevens was voorzien.

Daarentegen oordeelde het Grondwettelijk Hof dat de Inlichtingenwet dat de inlichtingsdiensten toegang geeft tot bewaarde communicatiegegevens wel conform de HvJ-rechtspraak is.[47] Immers, artikel 18/3 Inlichtingenwet geeft de inlichtingendiensten enkel toegang tot bewaarde gegevens indien er een ernstige potentiële dreiging bestaat en gewone methoden voor het verzamelen van gegevens ontoereikend zijn. Deze bepaling beperkt dus reeds de toegang tot deze gegevens tot wat strikt noodzakelijk is in lijn met de filosofie van de Luxemburgse dataretentie-rechtspraak. Het GwH ondersteunde daarbij het onderscheid dat Luxemburg maakt tussen retentie voor de bescherming van de nationale veiligheid en de strijd tegen ernstige criminaliteit door te wijzen op het verschil in finaliteit, zijnde het concrete gebruik van de gegevens:

45 GwH 22 april 2021, nr. 57/2021, www.const-court.be. Over dit arrest Cécile De Terwangne, "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", *Rev.trim.DH*, vol 129 (2022): 3-27; Liesa Keunen, "Bewaren van elektronische communicatiegegevens: de uitzondering en niet de regel", *NJW*, vol. 454 (2022): 30; Oerlemans, Hagens en Royer, "Tijd voor een nieuwe bewaarplicht?", 152 – 154; De Keersmaecker en Van de Heyning, "De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga", 171; Jan Janssen, "Bewaren of beware : dataretentie en grondrechten, een moeilijk evenwicht", *RABG*, vol. 8 (2021): 673; Julie Petersen, "Lang verwacht en zoals gedacht, het Grondwettelijk Hof vernietigt de dataretentiewet", *RABG*, vol.11 (2021): 1007.

46 GwH 22 april 2021, nr. , § B.24.1 – 24.2.

47 GwH 22 april 2021, nr. 64/2021. Het Hof werd hierbij in het bijzonder bevraagd over de bewaring van de communicatiegegevens van personen met een professionele vertrouwelijkheid zoals dokters en advocaten. Het GwH meende dat deze retentie verantwoord was in het licht van de bescherming van de nationale veiligheid.

> "De zoektocht naar gegevens in het kader van een opsporings- of gerechtelijk onderzoek is erop gericht bewijselementen te verzamelen met betrekking tot een misdrijf, die daadwerkelijk bruikbaar zijn in een strafprocedure voor de rechter ten gronde. De gegevens die de inlichtingen- en veiligheidsdiensten verzamelen, strekken niet ertoe een rechter ten gronde te overtuigen van de strafrechtelijke "schuld" van een beklaagde, maar wel de overheid toe te laten de noodzakelijke maatregelen te nemen ter vrijwaring van de fundamentele belangen van het land." (r.o. B.10.1)

Het GwH wees bijkomend op de garanties voor de bescherming van persoonsgegevens en privacy die in de Inlichtingenwet zijn opgenomen. Deze wet voorziet namelijk in een rapportering over de redenen van de toegang alsook tot welke gegevens toegang wordt genomen. Het Comité I moet hiervan onverwijld op de hoogte gebracht waardoor controle door een onafhankelijke bestuurlijke autoriteit mogelijk is. De termijn van toegang is bovendien beperkt en een verlening van de termijn kan op basis van artikel 18/8 § 2 wordt beoordeeld op basis van de ernst van de dreiging voor de nationale veiligheid waarvoor de gegevens worden opgevraagd. De toegang tot deze gegevens is daardoor voor de inlichtingendiensten veiliggesteld, maar in de praktijk zullen ze over veel minder gegevens beschikken aangezien de bepaling die een algemene retentie van identificatie - , locatie – en verkeersgegevens voorzag, vernietigd werd.

Als gevolg van de vernietiging van de dataretentiewet 2016 geldt er geen algemene dataretentieverplichting meer voor operatoren en diensten van elektronische communicatie. Deze gegevens mogen nog wel bijgehouden worden op basis van artikel 5 van de E-privacy richtlijn, namelijk de gegevens die met toestemming van het data-subject werden bewaard (*consent-based*), gegevens die worden bijgehouden voor de transmissie van de communicatie (technische redenen), en gegevens die worden bijgehouden voor de facturatie, marketing of diensten met toegevoegde waarde (zogenaamde *business purpose*). Deze gegevens mogen maar worden bijgehouden zolang als nodig voor de doelstelling. Daardoor zijn voor enkele weken tot maanden deze gegevens nog wel aanwezig. Zoals bleek uit de HvJ-rechtspraak mogen de vervolgende en rechterlijke instanties alsook de inlichtingendiensten wel toegang nemen tot deze gegevens voor de bestrijding van criminaliteit, bescherming van de openbare orde en nationale veiligheid. Dit zal in grote mate reeds tegemoetkomen aan de noodzaak in bevraging van dergelijke gegevens. Immers, uit de publiek beschikbare cijfers van de BIPT blijkt dat een zwaartepunt voor de bevraging van deze gegevens ligt in de eerste drie maanden van de creatie en dus bewaring van deze gegevens.[48]

Opvraging	*< 3 maanden*	*Tussen 3 – 6 maanden*	*Tussen 6 - 9 maanden*	*Tussen 9 – 12 maanden*	*> 12 maanden*
2014	51.921	15.961	7299	12.396	/
2015	56.466	15.172	5558	11.010	/
2016	196 522	20 782	9 797	12 659	/
2017	328.330	70.861	51.405	339.094	58.355
2018	314.432	61.487	39.453	441.177	68.893

48 BIPT, Statistische inlichtingen inzake dataretentie, te raadplegen: https://www.bipt.be.

Deze cijfers laten echter ook zien dat er vele gegevens worden bevraagd in de laatste drie maanden van de huidige bewaring, namelijk tussen de 9de en 12de maand. De kans bestaat dat op dat moment geen gegevens meer beschikbaar zijn. Uit een bevraging van de autoriteiten in opdracht van de Europese Commissie bleek daarbij dat in het bijzonder landen zonder een algemene retentie vervolgende autoriteiten aangeven dat de bewaartermijnen vaak onvoldoende zijn om de online-aspecten van misdrijven te onderzoeken, onder andere in onderzoeken naar seksuele uitbuiting van minderjarigen, kindermisbruikmateriaal of cyberaanvallen, of om onderzoek te doen naar complexe georganiseerde misdaad, die vaak pas veel later ontdekt wordt.[49] Daardoor zouden bepaalde misdrijven in deze lidstaten minder vervolgd worden.[50]

De huidige situatie stimuleert bovendien onderzoekers om zo snel mogelijk gegevens op te vragen omdat deze maar tijdelijk beschikbaar zijn. Bovendien is het niet duidelijk hoelang de operatoren en dienstverleners van elektronische communicatienetwerken deze gegevens bewaren aangezien hierover geen transparantieverplichting bestaat en elk bedrijf een ander beleid hieromtrent heeft. Dit houdt het risico in dat onderzoekers standaard deze gegevens zouden opvragen in het strafonderzoek zonder een grondige analyse of deze gegevens wel nodig zijn voor het onderzoek en dus een inbreuk op de privacy en persoonsgegevens verantwoorden uit vrees dat deze gegevens niet meer beschikbaar zouden zijn als later zou blijken dat ze noodzakelijk zijn. De korte bewaring is daardoor een tweesnijdend zwaard: de korte termijn zorgt voor een beperktere inbreuk op de privacy en bescherming van persoonsgegevens maar daardoor is er meer incentive om deze gegevens snel te bevragen wat dan weer een negatieve impact heeft op deze rechten.

Een nieuwe wet dient zich aan

Intussen werd een nieuw voorstel voor dataretentiewet in de commissie justitie van het parlement voorgelegd.[51] Het nieuwe artikel 126 van de wet elektronische communicatie combineert een algemene retentie van identificatiegegevens voor een periode van 12 maanden met een gerichte bewaring van locatie – en verkeersgegevens op basis van bewaringsbevelen. Daarbij voorziet artikel 126 ten eerste een nieuwe regeling waarbij een algemene retentie geldt voor bepaalde zones waar er een hogere dreiging op ernstige criminaliteit bestaat, namelijk:

- de gerechtelijke arrondissementen waar per jaar per 1000 inwoners minstens 3 strafbare feiten die gekwalificeerd worden als misdrijven in de zogenaamde taplijst in artikel 90ter § 2 en § 4 van het Wetboek van Strafvordering zijn vastgesteld;
- de politiezones waar per 1000 inwoners over een gemiddelde van de afgelopen 3 jaar voorafgaand aan het bewaarbevel minstens drie strafbare feiten die gekwalificeerd worden als misdrijven in de zogenaamde taplijst in artikel 90ter § 2 en § 4 van het Wetboek van Strafvordering zijn vastgesteld.

49 Milieu ltd studie voor de Europese Commissie, Study on the retention of electronic communications non-content data for law enforcement purposes, (Luxemburg: Publications Office of the European Union, 2020).

50 Daarentegen bleek uit een rapport van het Duitse Openbaar Ministerie dat dataretentie nauwelijks impact zou hebben op het oplossen van lopende strafonderzoeken. Moritz Campino Wolf en Daniël Wurst, "Einsatz digitaler Technologien durch staatliche Akteure in Demokratien und autokratischen Staaten", te raadplegen: https://blogs.urz.uni-halle.de/informatikundgesellschaft/files/2021/10/Wolf_und_Wurst.pdf.

51 Wetsontwerp 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. 55-2572/001. Het Wetsontwerp werd ingediend op 17 maart 2022. Hierover: Sem Careel en Sofie Royer, "Voorontwerp dataretentiewet: derde keer, goede keer?", *Juristenkrant*, vol. 431 (2021): 10.

De bewaartermijn voor de gegevens (6, 9 of 12 maanden) is afhankelijk van het aantal vastgestelde misdrijven in de bewuste geografische zone. De Gegevensbeschermingsautoriteit bekritiseerde deze regeling omdat er geen transparante cijfers beschikbaar zijn over de mogelijke impact, namelijk hoeveel gerechtelijke arrondissementen of politiezones hierdoor onder deze maatregel van geografische retentie van locatie – en verkeersgegevens zouden vallen.[52] Deze regeling kan er in de praktijk toe leiden dat het nagenoeg het gehele grondgebied onder deze regeling valt, waardoor de nieuwe dataretentiewet tot een gelijkaardige bewaring zal leiden als de vernietigde wet.

Deze regeling lijkt *prima facie* conform de HvJ-rechtspraak aangezien deze de bewaring op basis van geografische zones toelaat, maar zou kunnen 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. Het wetsontwerp bepaalt dat de beoordeling gebeurt 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.

Ten tweede werd ook een nieuwe regeling uitgedokterd die een algemene retentie voor de bescherming van de nationale veiligheid toelaat in het geval van een ernstige, actuele en reële dreiging. Indien het dreigingsniveau zoals bepaald door het OCAD minstens niveau 3 bereikt, zullen de operatoren ingelicht worden dat ze moeten overgaan tot de bewaring van locatie – en verkeersgegevens over het gehele grondgebied. Deze bepaling lijkt overeenkomstig de HvJ-rechtspraak aangezien dit niveau slechts bereikt wordt bij een ernstige, mogelijke en waarschijnlijke dreiging. Deze bewaarplicht moet bevestigd worden bij koninklijk besluit binnen de maand na het bewaarbevel, wat de nodige transparantie met zich meebrengt.

Ten derde voorziet het ontwerp ook in een bewaringsverplichting van verkeer – en locatiegegevens in gebieden die bijzonder zijn blootgesteld aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, zoals luchthavens of gemeenten waar kritische infrastructuur gevestigd is, alsook zones waar een mogelijke ernstige dreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, bijvoorbeeld het parlement of gemeenten waar militaire domeinen zijn. Ook hier lijkt dit criterium op het eerste zicht in overeenstemming met de HvJ-rechtspraak, maar zal in de praktijk bekeken moeten worden of de retentie zich in gebied en gebruikers beperkt tot wat strikt noodzakelijk is. Hierbij zal rekening gehouden moeten worden met de technische mogelijkheden om een gerichte zone voor bewaring af te bakenen. Bijvoorbeeld is een retentie op basis van een bepaalde account of telefoonnummer veel gerichter dan retentie op basis van een zendmast.

In de wet wordt echter nog een bijkomende mogelijkheid voor langere retentie gebouwd. Artikel 122 wet elektronische communicatie wordt aangepast zodat operatoren en dienstverleners van elektronische communicatie langer communicatiegegevens mogen bewaren in het geval van vermeende fraude of kwaadwillig gebruik van het communicatienetwerk. Een langere bewaring is ook mogelijk voor verkeersgegevens die nodig zijn om de veiligheid en correcte werking van het communicatienetwerk – of dienst te garanderen, in het bijzonder in het geval van een aanslag op

52 Gegevensbeschermingsautoriteit, Advies nr. 108/2021 van 28 juni 2021 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), Parl.St. 55-2572, 720 (hierna Advies DPA dataretentiewet), 777.

dit netwerk. Op die manier zullen in het geval van ernstige cyberaanvallen op netwerken, zoals ransomware – of ddos - aanvallen nog gegevens voorradig zijn om deze te onderzoeken. De vraag stelt zich daarbij wat moet worden verstaan als fraude of kwaadwillig gebruik. Kan een dergelijke langere bewaring bijvoorbeeld gerechtvaardigd worden voor elektronische belaging zoals vervat in artikel 145 § 3bis van de wet elektronische communicatie of ander cybergeweld dan wel economische online fraude zoals phishing? In die lezing zou er een brede retentie mogelijk blijven voor locatie – en verkeersgegevens die gebruik zal worden in cybercrime onderzoeken.

Uit het ontwerp van wet is het duidelijk dat de regelgever een zo breed mogelijke bewaring van gegevens wil garanderen voor de strijd tegen ernstige criminaliteit en voor de bescherming van de nationale veiligheid, maar zich hierbij baseert op de criteria die door het HvJ werden aangereikt. De vraag stelt zich daarbij of deze criteria ook conform het doeltreffendheidsbeginsel van het recht van de Europese Unie werden toegepast. Berhélémy van de Liga voor Mensenrechten meende dat de overheid zoveel gebieden aanwijst als gevoelig of met grote kans op ernstige misdrijven dat dit *de facto* neerkomt op een bijna algemene gegevensbewaring.[53] Zonder twijfel zal ook deze tekst, eens het door het parlement gestemd word en door de koning bekrachtigd, voorgelegd worden aan het Grondwettelijk Hof en Hof van Justitie voor de beoordeling in het licht van de artikelen 7, 8 en 11 Handvest. Het is daardoor niet ondenkbaar dat de regelgever binnen enkele jaren zich opnieuw over het vraagstuk van dataretentie mag buigen.

Zonder twijfel het meest gecontesteerde deel van het wetsontwerp betreft de regels opgenomen in het nieuwe artikel 107/5 wet elektronische communicatie over de versleuteling van communicatie. Deze versleuteling wordt vandaag al veelvuldig toegepast op elektronische netwerken, omdat het communicatie beveiligd en het cybercriminelen of andere derden onmogelijk maakt om deze communicatie te volgen. Steeds meer Big Tech - bedrijven kiezen ervoor om communicatieapplicaties volledig te versleutelen. De nieuwe bepaling stelt als principe dat het gebruik van versleuteling vrij is om de digitale veiligheid te bevorderen. Dit artikel voorziet hier wel twee uitzonderingen op. Ten eerste mag het gebruik van versleuteling noodcommunicatie niet verhinderen, bv. voor het identificeren van de plaats van waar het noodsignaal kwam. Ten tweede mag deze versleuteling het niet onmogelijk maken voor operatoren en aanbieders van elektronische communicatie om te antwoorden op gerichte verzoeken van een bevoegde autoriteiten met als doel om een eindgebruiker te identificeren of niet publiek toegankelijke communicatie op te sporen en te lokaliseren.

De regering wil daarmee verhinderen dat alle communicatiegegevens nodig voor het opsporen van misdrijven of voor de bescherming van de nationale veiligheid achter de ondoordringbare deuren van versleuteling verdwijnen. De vraag is maar hoe dit zich in de praktijk zal vertalen, aangezien operatoren en dienstverleners niet op voorhand kunnen weten welke communicatie wel en welke niet bevraagd zal worden. Bovendien wordt beargumenteerd dat versleuteling criminaliteit voorkomt en de nationale veiligheid beschermt doordat derden, zoals cybercriminelen of buitenlandse spionagediensten, niet kunnen meelezen in de communicatie van personen of hun gegevens kunnen misbruiken.[54] De Gegevensbeschermingsautoriteit adviseerde negatief op dit punt door te oordelen dat deze beperkingen aan het gebruik van versleuteling "een onevenredige aantasting [vormt] van het recht op eerbiediging van het privéleven van de betrokkenen" en daardoor "verder [gaat] dan wat in een

53 Chloé Berthélémy, "New Belgian data retention law: a European blueprint?", EDRI 17 november 2021, te raadplegen: https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint.

54 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), te raadplegen: https://www.globalencryption.org.

democratische samenleving noodzakelijk is".[55] In de memorie van toelichting beantwoordt de minister van justitie deze kritiek door te stellen dat elke bewaarplicht onzinnig wordt als deze gegevens niet meer leesbaar en dus niet meer beschikbaar zijn. Zonder twijfel zal ook deze bepaling voer worden voor debat in het parlement en juridische procedures vanuit zowel de bescherming van het recht op privacy en persoonsgegevens als vanuit de Algemene Verordening Persoonsgegevens en de NIS-richtlijn voor de bescherming van essentiële diensten die versleuteling naar voor schuiven als een middel om een hogere beveiliging online te verzekeren.

De nabije toekomst: Europese incoherentie

Van privacy naar veiligheidsbesognes: een gewijzigde context

Toen het Hof van Justitie in de zaken *Tele2/Watson* oordeelde dat een algemene retentie van elektronische verkeer – en locatiegegevens in strijd was met het Unierecht en daardoor niet toegelaten, reageerden verschillende lidstaten en experten van vervolgende autoriteiten alsook inlichtingendiensten met ontsteltenis. Volgens hen bracht het Hof van Justitie met deze rechtspraak de veiligheid en strijd tegen criminaliteit in gevaar. Het antwoord op deze rechtspraak was dan ook voor de meeste lidstaten geen aanpassing van hun wetgeving in lijn met de Luxemburgse, maar een afwachtende houding. Verschillende hoogste rechtscolleges stuurden immers nieuwe prejudiciële vragen naar het HvJ over de mogelijkheden om alsnog gegevens te bewaren en deze te gebruiken. In enkele van deze prejudiciële vragen wordt het Hof erop gewezen dat er nog andere belangen en fundamentele rechten in het geding zijn dan de bescherming van privacy en persoonsgegevens, dewelke nu ondermijnd zouden worden door de dataretentie-rechtspraak.

Het Belgisch grondwettelijk hof, bijvoorbeeld, merkte in haar prejudiciële vragen op dat er op de lidstaten een positieve verplichting rustte om het recht op leven en integriteit van haar inwoners te beschermen en dit bemoeilijkt zou worden zonder dataretentie, bijvoorbeeld in zaken van kindermisbruik.[56] De Franse Conseil D'Etat benadrukte in haar prejudiciële vraag dan weer de uitdagingen voor de nationale veiligheid, in het bijzonder het terreurgevaar.[57] Het Irish Supreme Court,[58] tot slot, vroeg of een nationale rechter de werking in de tijd van de onverenigbaarheid van nationale dataretentie-regels met het Unierecht mag beperken indien hij ervan overtuigd is dat het niet-beperken in de tijd van die beslissing zou leiden tot "chaos en schade aan het algemene belang" (*An Garda Síochána* r.o. 30). Op deze vragen had het Hof van Justitie reeds geantwoord in haar arresten *Tele2/Watson*. De vragen konden dan ook niet anders geïnterpreteerd worden als een uitnodiging voor het Hof van Justitie om haar rechtspraak te herdenken.

Deze vragen getuigen bovendien van een shift in bezorgdheden over het privacy-beleid in het nationale veiligheidsbeleid. In de eerste prejudiciële vragen (*Digital Rights Ireland* en *Tele2/Watson*) lag de focus op de vraag of de nationale retentie van elektronische communicatiegegevens geen disproportionele inbreuk op het recht op privacy en persoonsgegevens uitmaakte. Toen het HvJ oordeelde over de verenigbaarheid van de dataretentierichtlijn en het Unierecht, hadden een aantal nationale hoogste rechtshoven al besloten dat deze richtlijn in strijd was met de nationale

55 Advies DPA dataretentiewet, 790.
56 GwH 19 juli 2018, nr. 96/2018.
57 CE 21 april 2021, nr. 393099, ECLI:FR:CEASS:2021:393099.20210421.
58 The Supreme Court 24 februari 2020, nr. 2019/18, te raadplegen: https://courts.ie/judgments.

bescherming van fundamentele rechten.[59] In de latere prejudiciële vragen, daarentegen lag de nadruk op de vraag of de door het HvJ gevonden evenwicht de strijd tegen ernstige criminaliteit en bescherming van de nationale veiligheid ondermijnde. De context waarbinnen de vragen werden gesteld, was dan ook danig gewijzigd. De eerste vragen werden beslist in de naweeën van surveillance schandalen, zoals de verregaande extraterritoriale toegang tot onze gegevens door de Amerikaanse inlichtingendiensten NASA die door Snowden wereldkundig werden gemaakt en de Cambridge Analytica – saga waaruit bleek hoe onze bewaarde gegevens misbruikt worden voor politieke doeleinden en de impact van dataretentie op fundamentele rechten en democratische waarden. [60] In de latere zaken werd het HvJ dan weer vooral geconfronteerd met de mogelijke impact op concrete veiligheidsdreigingen, zoals terrorisme, en ernstige criminaliteit, zoals kindermisbruik.

De zaak aan de oorsprong van het arrest noopte het Hof van Justitie tot een bijzonder moeilijke beslissing. Graham Dwyer werd in verband gebracht met een tot dan toe onopgeloste moord van een kinderverzorgster op basis van bewaarde verkeers- en locatiegegevens van telefoongesprekken. Dwyer voerde een jarenlange juridische strijd om de levenslange gevangenisstraf waartoe hij werd veroordeeld ongedaan te maken. Hij meende dat de zaak beruste op deze gegevens die in weerwil van het Unierecht waren bewaard, waardoor dit bewijs uitgesloten moest worden. Deze zaak was voor het Ierse hoogste gerechtshof een 'hard case' zoals Twining en Miers dit interpreteren, namelijk een zaak waar het recht duidelijk is, namelijk in strijd met het Unierecht, maar waar de rechter aanzienlijke bedenkingen heeft in de concrete zaak om deze principes toe te passen.[61] De kritische bewoordingen in de prejudiciële vraag van het Irish Supreme Court getuigen van deze gewijzigde context.

Het Hof van Justitie was niet blind voor deze kritiek en ging actief in op deze uitdagingen voor de nationale autoriteiten.[62] Het Hof bleek niet bereid om de fundamentele principes die het reeds in haar rechtspraak had vastgesteld te wijzigen, namelijk de vaststelling dat de strijd tegen ernstige criminaliteit geen algemene retentie van verkeer – en locatiegegevens verantwoordde. Daarentegen zorgde het wel voor verduidelijking en beperkte het de draagwijdte van haar rechtspraak in de toepassing om de nationale veiligheid en strijd tegen ernstige criminaliteit te vrijwaren. Deze heroverweging leidde tot de verduidelijking dat IP-gegevens die een persoon of toestel identificeren, ongedifferentieerd bewaard mogen worden, dat een algemene retentie van verkeer – en locatiegegevens wel mogelijk is voor de nationale veiligheid in het geval van een ernstige, actuele en reële dreiging, dat een *quick freeze* van deze gegevens voor de strijd tegen ernstige criminaliteit mogelijk is,[63] of nog, dat lidstaten een algemene retentie mogen toelaten voor bepaalde geografische zones op basis van gemiddelde criminaliteitscijfers. Deze beperkingen van de eerder vastgestelde principes tonen dat het Hof van Justitie in gesprek met de hoogste rechtscolleges naar een duurzaam evenwicht zoekt. Deze laatste arresten zullen echter de regelmatige vragen aan het Hof over dataretentie niet stoppen.

59 Vainio en Miettinen, "Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States", 290–309.

60 Humble merkt op dat de impact van deze schandalen vooral gevoeld werd in de regionale bescherming van privacy dan op het internationale vlak bij gebrek aan een internationaal aanvaard concept van privacy in de digitale sfeer. Kristian Humble, "Human rights, international law and the right to privacy", The International Journal of Human Rights 2021, vol. 23, nr. 12 (2021): 14 – 23.

61 William Twining en David Miers, *How to do Things with Rules* (Londen: Weidenfeld and Nicolson, 1991).

62 Catherine Van de Heyning, "Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog", *T.Strafr.*, vol. 2 (2019): 86; Jan Podkowik, Robert Rybski en Marek Zubik, "Judicial dialogue on data retention laws: A breakthrough for European constitutional courts?", *International Journal of Constitutional Law,* vol. 19, nr. 5 (2021): 1597 - 1631.

63 Naast de algemene bewaring van identificatie – en ip – gegevens, aanvaardde het HvJ eveneens dat lidstaten konden overgaan tot een snelle algemene bewaring van gegevens in strijd tegen ernstige criminaliteit alsook een automatische analyse van gegevens voor de bescherming van de nationale veiligheid. Hierover uitgebreid in De Keersmaecker en Van de Heyning, "De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga", 171.

De Belgische wet is een voorbeeld van hoe de lidstaten binnen de vooropgestelde criteria een nieuwe poging doet om een brede retentie van verkeer – en locatiegegevens te bewerkstelligen, wat zonder twijfel opnieuw door het Hof van Justitie zal getoetst worden.

Het kritische punt van deze discussie is dat het Hof, maar ook de nationale autoriteiten, in deze discussie in hoge mate blind varen. Er zijn nagenoeg geen publieke cijfers beschikbaar die een duidelijk overzicht geven van welke gegevens hoe vaak bewaard worden en bevraagd worden door nationale autoriteiten, voor de strijd tegen ernstige criminaliteit of de nationale veiligheid. In een studie van 2020 in opdracht van de Europese Commissie over de nationale praktijken van dataretentie, schreven de auteurs over de vergelijking van de nationale cijfers over het opvragen van communicatiegegevens in strafzaken het volgende:

> "It can be concluded that cross-country comparisons are meaningless without a homogenous reporting system. Requests for non-content data are recorded in a variety of ways and the methodology used is often not clearly explained."[64]

Evenmin is er voldoende transparantie over de vraag hoe deze gegevens gebruikt werden of welke rol ze speelden: waren ze oriënterend bij aanvang van een onderzoek om een mogelijke verdachte te vinden, waren ze belangrijk of doorslaggevend bewijs van de schuld van een persoon of betrokkenheid bij potentiële veiligheidsdreigingen, of werden de gegevens bewarend opgevraagd in het licht van de korte retentietermijnen en daardoor ook regelmatig niet gebruikt. Tot slot is er ook weinig duidelijkheid over hoe vaak de opgevraagde gegevens ook nuttige informatie opleverden. Bijvoorbeeld kan je IP-adressen opvragen, maar kan hieruit blijken dat het om een publiek adres gaat waar zeer vele gebruikers zich op bevonden waardoor niets uit de gegevens kan afgeleid worden. Anders gezegd, welke rol de opgevraagde gegevens werkelijk in de strijd tegen criminaliteit en nationale veiligheid spelen, is onvoldoende duidelijk in publieke gegevens. En verder, welke onderzoeken konden niet verdergezet worden omdat er geen gegevens beschikbaar waren in navolging van de HvJ-rechtspraak. Professionelen in vervolgende instanties zullen benadrukken dat deze in het merendeel van de strafonderzoeken van belang zijn, maar concrete cijfers en meer kennis alsook gebruik van deze gegevens zijn nodig zijn om een eventuele shift in de HvJ-rechtspraak te bewerkstelligen.[65] Transparantieverplichtingen voor zowel de operatoren en dienstverleners van elektronische communicatienetwerken als voor autoriteiten zou daarom een grote meerwaarde zijn voor het debat.

De korte termijn: Europese incoherentie

De lidstaten reageerden zeer verschillend op de Europese rechtspraak. Een aantal landen legden zich neer bij het nieuwe evenwicht zoals het Hof van Justitie dit uitwerkte of namen een afwachtend houding aan na de vernietiging of terzijdestelling van de nationale regelgeving. Nadat de Nederlandse Wet bewaarplicht telecommunicatiegegevens buiten werking werd gesteld in navolging van het *Digital Rights*

64 Vrije vertaling: "Geconcludeerd kan worden dat vergelijkingen tussen landen zinloos zijn zonder een homogeen rapportagesysteem. Verzoeken om niet-inhoudelijke gegevens worden op verschillende manieren gemeten en de gebruikte methode wordt vaak niet duidelijk uitgelegd". Milieu ltd studie voor de Europese Commissie, *Study on the retention of electronic communications non-content data for law enforcement purposes*, 62.

65 Openbare aanklagers gaven aan in 60 tot 80% van de strafonderzoeken dergelijke cijfers op te vragen, maar ook hier ontbreekt het in de lidstaten aan transparante cijfers. Milieu ltd studie voor de Europese Commissie, *Study on the retention of electronic communications non-content data for law enforcement purposes*, 63. Daar tegenover staan de inschatting van het Duitse openbaar ministerie dat met een algemene dataretentie nauwelijks meer zaken opgelost zouden worden.

Ireland – arrest[66] werd nog geen nieuwe wetgeving aangenomen voor de verplichte bewaring van communicatiegegevens. De telecommunicatiewet voorziet wel in een mogelijkheid, geen verplichting, om dergelijke gegevens te bewaren. Op basis van artikel 11.13 Telecommunicatiewet kunnen aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten elektronische communicatiegegevens bewaren voor de nationale veiligheid of strijd tegen ernstige criminaliteit. Er is reeds verschillende jaren een voorstel hangende in het Nederlandse parlement om een verplichte retentie te voorzien voor zogenaamde gebruikersgegevens.[67] Volgens Oerlemans, Wagemans en Royer zou een dergelijk voorstel in overeenstemming zijn met de recente arresten.[68] De Nederlandse wetgever zal bovendien het Wetboek voor Strafvordering bijkomend moeten aanpassen voor wat de toegang tot deze gegevens betreft. In een arrest van 5 april 2022 bevestigde de Hoge Raad dat de huidige procedure in 126n en 126ng Wetboek van Strafvordering niet in overeenstemming is met de rechtspraak van het Hof van Justitie en de fundamentele rechten, omdat de officier van justitie ook gericht bewaarde locatie – en verkeersgegevens kan opvragen. Dit kan volgens de Hoge Raad enkel via de rechter-commissaris die de rechten en belangen ook effectief moet toetsen en verantwoorden.[69]

Ook in verschillende andere landen zoals Duitsland, Oostenrijk en Slovenië werden 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.[70] De Duitse minister van justitie ging intussen een stap verder en kondigde aan dat Duitsland een algemene dataretentie volledig zou afschaffen, en dus ook voor identificatiegegevens.[71] Duitsland zou daarmee een stap verder gaan dan andere lidstaten. Dat wil niet zeggen dat nationale autoriteiten niet meer over gegevens kunnen beschikken. Operatoren en dienstverleners van elektronische communicatie mogen wel nog gegevens bijhouden op basis van toestemming, technische doelstellingen of *business purpose*. Dit volgt nadat Advocaat-Generaal Campos Sanchez-Bordona van het Hof van Justitie in zijn opinie al aangaf dat de Duitse regelgeving over de bewaring van elektronische communicatiegegevens in strijd was met het Unierecht doordat het de algemene bewaring van locatie – en verkeersgegevens toelaat.[72] Op basis van de eerdere rechtspraak wist Duitsland dus al dan een quasi-zekere veroordeling door het HvJ op korte tijd zou volgen. Deze opinie maar ook een andere politieke wind deed de Duitse regering beslissen om nog voor een mogelijke veroordeling haar dataretentie beleid volledig om te gooien.

Andere lidstaten daarentegen bekijken hoe ze alsnog een brede retentie van elektronische communicatiegegevens kunnen verzekeren, zij het op basis van de criteria vooruitgeschoven door het Hof van Justitie. De Franse regering ging zelfs zo ver om de Conseil d'Etat op te roepen het arrest *La Quadrature du Net* naast zich neer

66 Rb. Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498.

67 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), Kamerstukken II 2015/16, 34537, nr. 2. Het originele voorstel werd na de arresten Tele2/Watson reeds aangepast en is nog steeds in bespreking op het moment van publicatie.

68 Oerlemans, Hagens en Royer, "Tijd voor een nieuwe bewaarplicht?", 157.

69 Hoge Raad 5 april 2022, nr. 21/04869, ECLI:NL:HR:2022:475

70 Voor een overzicht van de verschillende EU-lidstaten zie Marek Zubik, Jan Podkowik en Robert Rybski, *European Constitutional Courts towards Data Retention Laws.*

71 Julia Emmrich en Jochem Gaugele, "Buschmann: Niemand soll gegen seinen Willen geimpft werden" (interview), *WAZ* 21 december 2021. De minister meende: "Ich lehne die anlasslose Vorratsdatenspeicherung ab und möchte sie endgültig aus dem Gesetz streichen. Sie verstößt gegen die Grundrechte. Wenn jeder damit rechnen muss, dass vieles über seine Kommunikation ohne Anlass gespeichert wird, dann fühlt sich niemand mehr frei". Vrije vertaling:" Ik weiger het bewaren van gegevens zonder concrete verantwoording en wil het definitief uit de wet halen. Het schendt grondrechten. Als iedereen er rekening mee moet houden dat er veel over hun communicatie wordt opgeslagen zonder reden, dan voelt niemand zich meer vrij".

72 Opinie AG Campos Sánchez-Bordona, Gevoegde Zaken C-793/19 en C-794/19, Space Net en Telekom Deutschland, ECLI:EU:C:2021:939.

te leggen. Volgens de Franse eerste minister ondermijnden de principes van de "sauvegarde des intérêts fondamentaux de la Nation, de prévention des infractions et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme, composante de l'objectif de valeur constitutionnelle de protection de l'ordre public ».[73] De Conseil d'Etat ging hier niet op in wijzend op de primauteit van het Unierecht.[74] Advocaat-Generaal Campos Sanchez-Bordona waarschuwde lidstaten al "af te zien van enige poging om een algemene en ongedifferentieerde opslag van alle verkeers- en locatiegegevens voor te schrijven".[75]

In elk geval is het duidelijk dat de verschillende lidstaten andere opties overwegen, waarbij sommigen algemene retentie definitief achter zich laten, terwijl anderen bekijken wat er nog te reden valt om voldoende bewaarde gegevens te verzekeren. Intussen werden reeds verschillende bestaande regelgevingen vernietigd door nationale rechtscolleges, waardoor het in vele lidstaten momenteel onduidelijk is wat de status van dataretentie is en in welke mate de operatoren en dienstverleners de reeds bewaarde gegevens nog moeten bewaren. Deze periode van onzekerheid alsook de verscheidenheid in nationale dataretentie-regelingen zijn slecht nieuws voor de grensoverschrijdende samenwerking in strafzaken binnen de Europese Unie.[76] Op basis van het Europees Onderzoeksbevel[77] kunnen nationale vervolgingsautoriteiten versneld identificatiegegevens uitwisselen. Waar voorheen nagenoeg elke lidstaat deze gegevens verplicht liet bewaren door operatoren en dienstverleners van elektronische communicatie, maakt het huidige lappendeken-beleid voor dataretentie dat vele verzoeken nutteloos zullen blijken. Een goed overzicht over de verschillende dataretentie-regimes is dan ook noodzakelijk voor een goede werking van dit instrument.

Deze verscheidenheid in nationale regelgeving bemoeilijkt bovendien het beleid van operatoren en dienstverleners van elektronische communicatienetwerken. Veelal bieden zij hun diensten aan in verschillende lidstaten en hebben zij een EU-wijd beleid voor de bewaring van gegevens. Deze moeten zij herzien en afstemmen op heel diverse nationale regelgevingen, wat grensoverschrijdende diensten zal bemoeilijken. Dit betekent zonder twijfel ook een volgende horde voor het Europese e-evidence voorstel.[78] Dit voorstel had het mogelijk moeten maken dat nationale autoriteiten rechtstreeks communicatiegegevens konden opvragen van operatoren en dienstverleners van elektronische netwerken, waar deze ook in de Europese Unie gevestigd zijn. Het voorstel kreeg reeds veel tegenwind zowel vanuit privacy-exper-

73 Vrije vertaling: "bescherming van de fundamentele belangen van de natie, het voorkomen van strafbare feiten en het opsporen van daders van strafbare feiten en de bestrijding van terrorisme, dewelke onderdeel is van de doelstelling van constitutionele waarde van de bescherming van de openbare orde". Conseil d'Etat 21 april 2021, nr. 393099, 394922, 397844, 397851, 424717, 424718, te raadplegen: www.conseil-etat.fr, ECLI:FR:CEASS:2021:393099.20210421.

74 De Franse Conseil d'Etat legde het arrest uit op een manier dat locatie – en verkeersgegevens die op een algemene wijze voor de nationale veiligheid werden bewaard ook gebruikt kunnen worden het onderzoek naar ernstige strafrechtelijke feiten. CE 21 april 2021, nr. 393099, 394922, 397844, 397851, 424717, 424718, ECLI:FR:CEASS:2021:393099.20210421, te raadplegen: www.conseil-etat.fr). Hierover : De Terwangne, "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", 3-27. Deze visie werd intussen door het HvJ in de zaak *An Garda Síochána* onderuit gehaald. Intussen vernietigde het Conseil Constitutionnel de Franse bepaling die een algemene retentie van locatie – en verkeersgegevens toeliet (Conseil Constitutionnel 11 maart 2022, nr. 2021-980, ECLI : FR : CC : 2022 : 2021.980.QPC).

75 Opinie AG Campos Sánchez-Bordona, Gevoegde Zaken C-793/19 en C-794/19, Space Net en Telekom Deutschland, ECLI:EU:C:2021:939, r.o. 49.

76 Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime (Brussel, 6 juni 2019), 10083/19.

77 Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken, OJ L-130.

78 Voorstel tot verordening van het Europees Parlement en de raad betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken COM(2018) 225 final, 2018/0108(COD). Stanislaw Tosza, "The European Commission's Proposal on Cross-Border Access to E-Evidence. Overview and Critical Remarks", Eucrim vol. 4 (2018): 212 – 219; Gavin Robinson, "The European Commission's e -Evidence proposal", Eur. Data. prot. L. Rev., nr. 3 (2018): 351.

ten als vanuit experten die wezen op de teruglopende bescherming van de rechtstaat en fundamentele rechten in verschillende lidstaten, zoals Hongarije en Polen.[79] Een zeer verscheiden nationale wetgeving over de retentie van elektronische communicatiegegevens zou wel eens de doodsteek van dit voorstel kunnen zijn. Om deze samenwerking op lange termijn te garanderen, is het niet uitgesloten dat de Europese Commissie opnieuw een initiatief neemt voor een grotere coherentie te verzekeren.[80] De tijd is zeker nog niet aangebroken aangezien er nog prejudiciële zaken hangende zijn en nieuwe regelgeving in ontwikkeling is die zonder twijfel ook door het Hof van Justitie getoetst zal worden. De Belgische wetgeving is in die zin een nieuwe testcase voor de toekomst van dataretentie in de Europese Unie.

Conclusie

De discussie over het bijhouden en gebruik van elektronische communicatiegegevens beroerde de laatste jaren de gemoederen. Nationale rechtscolleges en het Hof van Justitie stonden voor de moeilijke taak 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. Het Hof van Justitie had in het arrest *La Quadrature du Net* gehoopt dat evenwicht te vinden door een principieel verbod op algemene retentie van locatie – en verkeersgegevens voor de strijd tegen criminaliteit te combineren met het toelaten van gerichte retentie van deze gegevens, en een algemene retentie van locatie – en verkeersgegevens voor de bescherming van de nationale veiligheid. De verscheidenheid van antwoorden door de nationale overheden op deze rechtspraak alsook de nog hangende prejudiciële vragen geven aan dat deze discussie zeker nog niet ten einde is. Waar het debat nog al teveel gevoerd wordt op argumenten dat ofwel elke vorm van dataretentie een disproportionele schending van de privacy is ofwel elke beperking van dataretentie de strijd tegen criminaliteit onmogelijk maakt, zouden transparante cijfers over het gebruik van deze gegevens een grote meerwaarde voor het debat kunnen betekenen. Wil een lidstaat dus het debat een andere richting insturen, zal het hierop moeten inzetten. ●

79 Sergio Carrera, Marco Stefan en Valsamis Mitsilegas, "Cross-border data access in criminal proceedings and the future of digital justice: Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic" (2020): 54 - 61, te raadplegen: https://www.ceps.eu ;Theodore Christakis, "E-evidence: the way forward (Summary of the Workshop held in Brussels on 25 September 2019)", te raadplegen: https://europeanlawblog.eu.

80 Zo werd onder andere bekeken of een aanpassing van de E-privacy richtlijn dataretentie zou mogelijk maken. Rojszcak, "The uncertain future of data retention laws in the EU: Is a legislative reset possible?"

BIBLIOGRAFIE

- Advies DPA dataretentiewet.
- Berthélémy, Chloé. "New Belgian data retention law: a European blueprint?". EDRI 17 november 2021, te raadplegen: https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint.
- BIPT. *Statistische inlichtingen inzake dataretentie,* te raadplegen: https://www.bipt.be.
- Brkan, Maja. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning". *German Law Journal*, nr. 20 (2019): 871 – 874.
- Campino Wolf, Moritz en Wurst, Daniël. "Einsatz digitaler Technologien durch staatliche Akteure in Demokratien und autokratischen Staaten". te raadplegen: https://blogs.urz.uni-halle.de/informatikundgesellschaft/files/2021/10/Wolf_und_Wurst.pdf.
- Campos Sánchez-Bordona. Gevoegde Zaken C-793/19 en C-794/19, *Space Net en Telekom Deutschland*, ECLI:EU:C:2021:939, r.o. 49.
- Campos Sanchez-Bordona. 18 november 2021, Zaak C-140/20, The Commissioner of the Garda Síochána, ECLI:EU:C:2021:942, r.o. 51.
- Careel, Sem en Royer, Sofie. "Voorontwerp dataretentiewet: derde keer, goede keer?". *Juristenkrant* 2021, vol. 432 (2021): 10.
- Carrera, Sergio; Stefan, Marco en Mitsilegas, Valsamis. "Cross-border data access in criminal proceedings and the future of digital justice: Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic." *CEPS Report* (2020): 54 – 61.
- CE 21 april 2021, nr. 393099, ECLI:FR:CEASS:2021:393099.20210421.
- Christakis, Theodore. "E-evidence: the way forward (Summary of the Workshop held in Brussels on 25 September 2019)". te raadplegen: https://europeanlawblog.eu.
- Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime (Brussel, 6 juni 2019), 10083/19.
- Conseil Constitutionnel 11 maart 2022, nr. 2021-980, ECLI : FR : CC : 2022 : 2021.980.QPC.
- Conseil d'Etat 21 april 2021, nr. 393099, 394922, 397844, 397851, 424717, 424718, te raadplegen: www.conseil-etat.fr, ECLI:FR:CEASS:2021:393099.20210421.
- Conings, Charlotte. *Klassiek en digitaal speuren naar strafrechtelijk bewijs*. (Antwerpen: Intersentia, 2017).
- Conings, Charlotte. "Dataretentie en privacy". *NJW*, afl. 333 (2015): 911 – 912.
- Conings, Charlotte en De Schepper, Kristel. "Dataretentie: tweede keer, goede keer", *Juristenkrant* (2016): 12
- Daeninck, Philip. *Telefonieonderzoek in het strafrecht - Het triumviraat van de artikelen 46bis, 88bis en 90ter Sv.,* (Brugge: Die Keure, 2021)

- De Keersmaecker, Robrecht en Van de Heyning, Catherine. "De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga", *T.Strafr*, nr. 4 (2021)
- De Smet, Bart. "Nieuwe regels voor dataretentie van telecomoperatoren: een obstakel voor de waarheidsvinding?", *RW*, vol. 11 (2016): 402.
- De Terwangne, Cécile. «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». *Rev.trim.DH*, vol 129 (2022) : 3-27.
- EHRM 25 mei 2021, *Big Brother Watch e.a. t. Verenigd Koninkrijk.*
- Emmrich, Julie en Gaugele, Jochem. "Buschmann: Niemand soll gegen seinen Willen geimpft werden" (interview), *WAZ* 21 december 2021.
- Facebook transparency report: https://transparency.fb.com/data/government-data-requests/country/BE/.
- Forget, « L'obligation de conservation des «métadonnées», la fin d'une longue saga juridique?», *JT* (2017).
- Gegevensbeschermingsautoriteit, Advies nr. 108/2021 van 28 juni 2021 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), Parl.St. 55-2572, 720 (hierna Advies DPA dataretentiewet), 777.
- 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), te raadplegen: https://www.globalencryption.org.
- Google transparency report: https://transparencyreport.google.com/
- GwH 11 juni 2015, nr. 84/2015, NC 2015.
- GwH 18 november 2021, nr. 158/2021.
- GwH 19 juli 2018, nr. 96/2018.
- GwH 22 april 2021, nr. 64/2021.
- GwH 22 april 2021, nr. 57/2021.
- Henrotte, "L' invalidation de la directive 2006/24 sur la conservation des données de communication électronique ou la chronique d'une mort annoncée". *JLMB* (2015): 956-957.
- HRM 25 mei 2021, *Centrum för Rättvisa t. Zweden*.
- Hoge Raad 5 april 2022, nr. 21/04869, ECLI:NL:HR:2022:475.
- Humble, Kristian. "Human rights, international law and the right to privacy". *The International Journal of Human Rights 2021*, vol. 23, nr. 12 (2021): 14 – 23.
- HvJ 2 maart 2021. Zaak C-7-46/18, Prokuratuur, ECLI:EU:C:2021:152.

- HvJ 2 oktober 2018, Zaak C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:788.
- HVJ 21 december 2016. zaak C-203/15 en C-698/15, *Tel2 Sverige AB t. Post - och telestryrelsen* en Secretary of state for the Home Department t. Tom Watson e.a., ECLI:EU:C:2016:970
- HvJ 5 april 2022. Zaak C-140/20, Commissioner of the Garda Síochána e.a, ECLI:EU:C:2022:258.
- HvJ 6 oktober 2020. Gevoegde zaken C-511/18, C-512 en C-520/18, La Quadrature du Net e.a., ECLI:EU:C:2020:791.
- HvJ 6 oktober 2020, Zaak C-623-17, Privacy International, ECLI:EU:C:2020:790.
- HvJ 8 april 2014, Zaak C-293/12 en 594, Digitial Rights Ireland Ltd. en Kärtner Landesregierung, ECLI:EU:C:2014:238.
- Janssen, Jan. "Bewaren of beware : dataretentie en grondrechten, een moeilijk evenwicht". *RABG*, vol. 8 (2021): 673.
- Jasserand, Catherine. "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?". *Computer Law & Security Review*, vol. 34, nr. 1 (2018): 154.
- Keunen, Liesa. "Bewaren van elektronische communicatiegegevens: de uitzondering en niet de regel". *NJW* 2022, vol. 454 (2022): 30.
- Klamberg, Mark. "Big Brother's little, more dangerous brother". Verbassungsblog 1 juni 2021, te raadplegen: https://verfassungsblog.de/raettvisa.
- Lynskey, Orla. " The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland". *Common Market Law Review*, afl. 6 (2014): 1789–1811.
- Mendos Kuskonmaz, Elif en Guild, Elspeth. "Rights-Based Review of Border Surveillance". *The Charter and the Court of Justice of the European Union: Notable Cases from 2016-2018* (Breda: Wolf Publishing 2019): 96.
- Milanovic, Marko. "The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa". *EJIL Talk!* 26 mei 2021, te raadplegen: www.ejiltalk.org
- Milieu ltd studie voor de Europese Commissie. *Study on the retention of electronic communications non-content data for law enforcement purposes* (Luxemburg: Publications Office of the European Union, 2020): 62.
- Murphy, Maria. "Data retention in the aftermath of Digital Rights Ireland and Seitlinger". *Irish Criminal Law Journal*, vol. 24, nr. 4 (2014).
- Oerlemans, Jan-Jaap; Hagens, Mireille en Royer, Sofie. "Tijd voor een nieuwe bewaarplicht?". *Computerrecht*, vol. 59 (2021): 152 – 154.
- Panzavolta, Michele; Royer, Sofie and Severijns, Helena. "Algemene dataretentie: ten minste houdbaar tot ...?", *T.Strafr*.afl. 1 (2018): 7 – 8.
- Petersen, Julie. "Lang verwacht en zoals gedacht, het Grondwettelijk Hof vernietigt de dataretentiewet", *RABG*, vol.11 (2021): 1007.
- Podkowik, Jan; Rybski, Robert en Zubik, Marek. "Judicial dialogue on data retention laws: A breakthrough for European constitutional courts?". *International Journal of Constitutional Law 2021, vol. 19, nr. 5 (2021): 1597 - 1631.*

— Rb. Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498.

— 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), Jur. L-201, 0037 – 0047.

— Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, Jur. L-105, 54–63.

— Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken, OJ L-130.

— Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, PB L 281 van 23.11.1995, 31.

— Roberts, Andrew. "Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications", *The Modern Law Review,* vol. 78, nr. 3 (2015): 535 – 548.

— Robinson, Gavin. "The European Commission's e -Evidence proposal", *Eur. Data. prot. L. Rev.*, nr. 3 (2018): 351.

— Rojszcak, Marcin. "The uncertain future of data retention laws in the EU: Is a legislative reset possible?". *Computer Law & Security Review 2021*, vol. 41, 05572 (2021).

— Royer, Sofie. "Dataretentie: Grondwettelijk Hof stelt prejudiciële vraag aan Hof van Justitie". *Computerrecht*, nr. 5 (2018): 247

— Royer, Sofie en Conings, Charlotte. "Ook hervormde dataretentiewet staat onder druk". *Juristenkrant*, iss 134 (2017): 1.

— Royer, Sofie en Careel, Sem. "Access denied – CJEU reaffirms la Quadrature du Net and clarifies requirements for access to retained data", *Citip Blog* 23 maart 2021, te raadplegen: www.law.kuleuven.be/citip/blog.

— Sajfert, Juraj. "Bulk data interception / retention judgments of the CJEU - A victory and a defeat for privacy". *European law blog* 26 oktober 2020, te raadplegen: https://europeanlawblog.eu.

— Sajfert, Juraj. "The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?". *European Law Blog* 8 juni 2021, te raadplegen: https://europeanlawblog.eu,

— Saugmandsgaard Øe 19 juli 2016, gevoegde zaken C-203/15 en C-698/15, Tele2 Sverige AB / Watson, ECLI:EU:C:2016:572, voetnoot 84.

— Supreme Court 24 februari 2020, nr. 2019/18, te raadplegen: https://courts.ie/judgments.

— Tosza, Stanislaw. "The European Commission's Proposal on Cross-Border Access to E-Evidence. Overview and Critical Remarks". *Eucrim* vol. 4 (2018): 212 – 219.

- Twining, William en Miers, David. *How to do Things with Rules* (Londen: Weidenfeld and Nicolson, 1991).
- Vainio, Niklas en Miettinen, Samuli. "Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States". *International Journal of Law and Information Technology*, vol. 23, nr. 3 (2015): 290–309.
- Van de Heyning, Catherine. "Data retention in Belgium", *European Constitutional Courts towards Data Retention Laws* (New York: Springer, 2021): 43 -74.
- Van de Heyning, Catherine. "Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog". *T.Strafr.* vol. 2 (2019): 86.
- Van de Heyning, Catherine. "Het gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek in gevaar?". *RABG*, iss 7 (2017): 533 – 538.
- Van de Heyning, Catherine. "Overzicht van rechtspraak – Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog", *T.Strafr.,* afl. 1 (2018): 38 – 47.
- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), Pub. L-119, 1 - 18.
- Verstraelen, Sarah. "De vernietiging van de Belgische datarententiewet met terugwerkende kracht: de bescherming van het privéleven primeert", *NC* (2015): 492-496.
- Wet van 13 juni 2005 betreffende de elektronische communicatie, BS 20 juni 2005, 28070.
- 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, 44717.
- 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 90decies van het Wetboek van Strafvordering, BS 23 augustus 2013, 56109.
- Wet van 30 november 1998 houdende regeling van de [inlichtingen- en veiligheidsdiensten, BS 18 november 1998, 40312.
- 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), Kamerstukken II 2015/16, 34537, nr. 2.