Hof van Justitie EU (Grote Kamer)
8 april 2014, gevoegde zaken C-293/12 en C-594/12
(Skouris (President), Lenaerts, Tizzano, Silva de Lapuerta, von Danwitz, Juhász, Borg Barthet, Fernlund, da Cruz Vilaça, Rosas, Arestis, Bonichot, Arabadjiev, Toader, Vajda)
Noot: M.E. Koning

Privacy. De eerbiediging van het privéleven en van het familie- en gezinsleven. De bescherming van persoonsgegevens. Bewaarplicht. Dataretentie. Nietigheid van de Dataretentierichtlijn. Proportionaliteit. Evenredigheid.

[Hv EU art. 7, 8; EVRM art. 8; Richtlijn 2006/24/EC art. 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 13; Richtlijn 95/46/EC art. 17; Richtlijn 2002/58/EC art. 4, 5, 6, 15]

Naar aanleiding van prejudiciële vragen gesteld in een nationaal geschil waarin onder meer de organisatie Digital Rights Ireland is betrokken, onderzoekt het HvJ EU of Richtlijn 2006/24/EG (de Dataretentierichtlijn) verenigbaar is met het Europese recht, in het bijzonder met Richtlijn 95/46/EG (de Gegevensbeschermingsrichtlijn) en met art. 7 en 8 Hv EU. Het Hof stelt voorop dat de Dataretentierichtlijn de lidstaten verplicht tot het bewaren van metadata over alle communicatie die plaatsvindt via telefonie of internet, d.w.z. waar het gaat om de bron en de bestemming van de communicatie, datum, tijdstip, duur en type communicatie, aard van het communicatiemiddel en locatie van mobiele telefonie. Daardoor is het mogelijk te identificeren welke personen met wie contact hebben gehad, op welk moment en op welke plaats, en daardoor kan ook worden bepaald met welke frequentie dat contact heeft plaatsgevonden. Dergelijke data geven in hun totaliteit een heel nauwkeurig beeld van het privéleven van de mensen wiens data worden bewaard. Daardoor kan bovendien enige impact bestaan op de vrijheid van meningsuiting als beschermd door art. 11 Hv, omdat mensen zich mogelijk weerhouden voelen van het benutten van communicatiemiddelen door de wetenschap dat de gegevens worden bewaard. In ieder geval is er sprake van een directe impact op de door art. 7 en 8 Hv beschermde rechten op privacy en databescherming, zodat moet worden bezien of daarvoor een voldoende rechtvaardiging bestaat in de zin van art. 52 Hv. Daarbij geldt dat het gaat om bijzonder ernstige inbreuken, nu mensen de indruk kunnen hebben dat zij onder voortdurend toezicht staan. Niettemin is hierdoor geen sprake van aantasting van de kern van art. 7 Hv, nu de inhoud van de communicatie niet wordt bewaard. Ook de kern van art. 8 Hv is niet aangetast nu er beperkingen zijn gesteld op de bewaring en opslag van de gegevens. Doelstelling van de regeling is het beschermen tegen criminaliteit en daarmee uiteindelijk bescherming van de veiligheid, wat in zichzelf een door art. 6 Hv beschermd individueel recht is. Aangenomen kan bovendien worden dat dataretentie een geschikt middel is om dit doel te realiseren. De vraag is niettemin of de regeling van dataretentie in de richtlijn een noodzakelijk middel is. In dit verband moet worden vastgesteld dat de intensiteit van de toetsing en de ruimte die de EU-wetgever heeft om over dit onderwerp regels te stellen, afhankelijk zijn van een aantal factoren, zoals in het bijzonder de aard van het aan de orde zijnde onderwerp, de aard van het betrokken grondrecht, de aard en ernst van de inbreuk en de nagestreefde doelstelling. Gelet op de belangrijke betekenis van de bescherming van data en de omvang en ernst van de daarop gemaakte inbreuk, moet hier een strikte toetsing worden uitgevoerd. Ten aanzien van de aan de noodzakelijkheid te stellen eisen betekent dit dat er duidelijke en nauwomschreven regels moeten worden vastgesteld met betrekking tot het bereik en de toepassing van de maatregelen in kwestie en dat er minimale waarborgen moeten worden ingebouwd die ervoor zorgen dat effectieve bescherming kan worden geboden tegen

misbruik en onrechtmatige toegang tot de gegevens. Het HvJ merkt bovendien op dat de maatregel in kwestie de gehele Europese bevolking raakt, zelfs personen waarvan op geen enkele manier bekend is dat zij een link hebben met ernstige criminaliteit en personen waarvan de communicatie wordt afgedekt door een beroepsgeheim. Ook zijn er geen beperkingen gesteld aan het bewaren van gegevens van bepaalde geografische zones, perioden in de tijd of kringen van personen. Kritisch is het Hof ook over het feit dat niet nader is gespecificeerd welke nationale autoriteiten toegang moeten kunnen hebben tot de gegevens en onder welke voorwaarden dat mag, waardoor niet is gegarandeerd dat zulke toegang is beperkt tot die gevallen waarin die strikt noodzakelijk is. De vastgelegde bewaartermijn tussen 6 en 24 maanden is niet door objectieve gronden gemotiveerd en daardoor evenmin beperkt tot wat strikt noodzakelijk is met het oog op het bereiken van de gestelde doelen. Gelet op deze overwegingen stelt het Hof vast dat de Dataretentierichtlijn de door art. 7, 8 en 52 Hv gestelde grenzen te buiten gaat en dat de richtlijn ongeldig is.

Digital Rights Ireland Ltd
tegen
Ierland

Noot

1. Deze uitspraak tekent zijn tijd. De documenten van klokkenluider Edward Snowden over de spionage- en surveillancepraktijken van zowel de Amerikaanse National Security Agency als verscheidene geheime diensten van lidstaten van de Europese Unie onthullen grootschalige en verregaande inbreuken op fundamentele rechten van EU-burgers. Deze surveillance wordt gedeeltelijk gekenmerkt door het verzamelen en het bewaren van telecommunicatie-metadata van burgers waartegen geen specifieke verdenking bestaat. Dit kenmerk vormt ook de kern van de verplichtingen die voortvloeiden uit de Dataretentierichtlijn.
2. In maart 2006 was de Dataretentierichtlijn aangenomen, maar deze is nu, acht jaar later, op 8 april 2014, met deze uitspraak door het HvJ EU nietig verklaard. De richtlijn eiste bewaring van telecommunicatie-metadata van vrijwel iedere EU-burger voor een periode van minimaal 6 tot maximaal 24 maanden. Met de metadata kunnen de volgende kernvragen over telecommunicatiegedrag worden beantwoord: tussen wie, met wat, waar, wanneer, op welke wijze en met welke middelen is er gecommuniceerd? Alleen de vraag "Waarom?" blijft onbeantwoord, want de bewaarplicht strekt zich niet uit tot de inhoud van telefoon- en internetspraakgesprekken en sms- en e-mailberichten.
3. Het is niet de eerste keer dat de richtlijn onderwerp is van een dispuut bij het HvJ EU. Het Hof sprak zich eerder al uit over de grondslag ervan in *Ierland t. Europees Parlement en Raad van de Europese Unie*, HvJ EU 10 februari 2009, zaak C-301/06, «JB» 2009/70 m.nt. Teunissen. Daarnaast heeft de bewaarplicht in de lidstaten zelf tot de nodige jurisprudentie geleid. In deze nationale zaken werd de implementatie van de richtlijn aan het evenredigheidsvereiste getoetst van lid 2 van artikel 8 EVRM en aan de eigen constitutionele bepalingen. Over de evenredigheid van de richtlijn zelf zwegen de nationale rechters. Zie voor overzichten van deze rechtspraak: C. Markou, 'The Cyprus and other EU court rulings on data retention: the Directive as a privacy bomb', *Computer Law & Security Review* 2012 (28), p. 468-475 en E. Kosta, 'The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection', 10 *SCRIPTed* 2013 (3), p. 339-363. Enkele

voorbeelden kunnen hier illustreren hoe op nationaal niveau over de richtlijn is geoordeeld.

4. Het Bulgaarse administratieve hof beoordeelde de privacyinbreuk van de implementatie van de richtlijn na een klacht van een privacybelangenorganisatie over de te ruim omschreven doelen, waarvoor toegang tot de metadata kon worden verkregen en de afwezigheid van waarborgen om de privacy te beschermen. Het Bulgaarse hof verklaarde de implementatie nietig omdat deze niet in beperkingen en waarborgen voorzag om de inbreuk op de privacy tot het minimale te begrenzen (Bulgaars administratief hof, 11 december 2008, nr. 13627). De legitimiteit van de essentie van de bewaarplicht of van de richtlijn bleef buiten beschouwing.

5. Het Roemeense grondwettelijk hof toetste ook naar aanleiding van een klacht van een burgerrechtorganisatie over de legitimiteit van de implementatie van de Dataretentierichtlijn. Dit grondwettelijk hof oordeelde dat de criteria in de nationale wet te vaag en weinig specifiek waren om een inbreuk op onder andere de privacy te legitimeren. Tevens legden de Roemeense rechters uit dat het constante en alles en ieder treffende karakter van de bewaarplicht de onschuldpresumptie omdraait en zo alle gebruikers van telecommunicatie op voorhand kwalificeert als verdachten van terroristische misdrijven of andere vormen van zware criminaliteit (Roemeens grondwettelijk hof, 8 Oktober 2009, nr. 1259). Hiermee deed het Roemeense hof uitspraak over de essentie van de bewaarplicht en dus indirect over de evenredigheid van de Richtlijn zelf, zonder zich de vingers te branden aan de verhouding tussen het EU-recht en de nationale constitutionele rechtsorde (vgl. C. Murphy, 'Note on Romanian Constitutional Court, Decision No. 1258 of 8 October 2009 regarding the unconstitutionality exception of the provisions of Law No. 298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of Law No. 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area', 47 *Common Market Law Review* 2010, p. 933-941).

6. Ook het Duitse federale grondwettelijk hof waagde zich niet aan een uitspraak over deze verhouding en wist zo "het openen van de doos van Pandora" met betrekking tot de verhouding van de nationale grondwettelijke hoven en het Hof in Luxemburg te voorkomen (Kosta, reeds aangehaald, p. 350; zie in dit verband ook C. DeSimone, 'Pitting Karlsruhe against Luxembourg? German data protection and the contested implementation of the EU Data Retention Directive', 11 *German Law Journal* 2010 (3), p. 291-317). Het Duitse hof stelde vast dat de toegang tot de bewaarde gegevens niet in de Richtlijn is geregeld en dat een lidstaat daarom een ruime discretionaire bevoegdheid toekomt (Bundesverfassungsgericht 2 maart 2010, *NJW* 2010, nr. 833). De bewaarplicht en de toegangscriteria konden daarom aan de eigen Grondwet worden getoetst zonder de achterliggende richtlijn aan fundamentele rechten te hoeven beoordelen, wat tot prejudiciële vragen aan het HvJ EU zou kunnen leiden.

7. Met deze redenatie haakte het hof in Karlsruhe aan op de eerdere uitspraak van het HvJ over de Dataretentierichtlijn van 10 februari 2009 (reeds aangehaald). In deze zaak betwistte Ierland de rechtsgrond (art. 95 EG-Verdrag (oud)) waarop de richtlijn was gebaseerd. Het HvJ wees op de mogelijkheid voor de toenmalige Gemeenschapswetgever om gebruik maken van de wetgevende procedure uit het oude art. 95 EG wanneer er verschillen zijn tussen nationale regelingen die de fundamentele vrijheden belemmeren of de mededinging verstoren. Voorafgaand aan de richtlijn verschilde de bewaarplicht per lidstaat en dit verstoorde de interne markt, aldus het HvJ (punten 63 en 71-72). Daarnaast wees het Hof erop dat de Europese richtlijn alleen de bewaring regelt bij de private partijen (punt 82). De regeling harmoniseert noch de toegang tot de gegevens door de

bevoegde nationale autoriteiten, noch het gebruik van die gegevens en de uitwisseling ervan tussen die autoriteiten (punt 83). De richtlijn bestrijkt zodoende geen maatregelen voor politiële en justitiële samenwerking in strafzaken, maar betreft enkel regulering van de interne markt. Om deze reden kon de bewaarplicht op Europees niveau in de eerste pijler worden geregeld en was een richtlijn, volgens het HvJ, hiervoor het aangewezen wetgevende instrument (punt 93).

8. Als gezegd liet het Duitse federale grondwettelijk hof de kwestie van rechtsgrond ongemoeid en beoordeelde het alleen de nationale implementatie van de richtlijn en de toegang tot deze gegevens op hun verenigbaarheid met de Duitse Grondwet. Het oordeelde dat de essentie van dataretentie op zichzelf genomen niet onconstitutioneel is, maar dat dataretentie wel een zwaarwegende inbreuk vormt op het recht tot vertrouwelijkheid van telecommunicatie (reeds aangehaald, r.o. 212). De vertrouwelijkheid van metadata over telecommunicatie wordt niet met zoveel woorden in Duitse Grondwet genoemd, maar het Bundesverfassungsgericht bevestigt dat dit onder artikel 10 van de Duitse Grondwet wordt beschermd (reeds aangehaald, r.o. 189).

9. Het feit dat de gegevens worden opgeslagen bij de private telecomproviders beschouwt het Bundesverfassungsgericht als een positief aspect dat de inmenging in de fundamentele rechten beperkt. Vervolgens onderwerpt het Bundesverfassungsgericht de toegangsaspecten van de Duitse bewaarplicht echter aan een strenge evenredigheidstoets, waarbij het toetst op de evenredigheid van de veiligheidswaarborgen, de proportionaliteit in verhouding tot de doelspecificatie en het verdere gebruik van de gegevens, de transparantie van de verwerking, en de beschikbaarheid van een daadwerkelijk rechtsmiddel en onafhankelijke toetsing van de maatregel (zie nader K. de Vries e.a., 'The German Constitutional Court judgement on data retention: Proportionality overrides unlimited surveillance (Doesn't it?)', in: S. Gutwirth, Y. Poullet, P. De Hert en R. Leenes (red.), *Computers, Privacy and Data Protection: an Element of Choice*, Dordrecht: Springer 2011, pp. 3-23). Het Bundesverfassunsgericht oordeelde dat de Duitse implementatie van de richtlijn op al deze punten te kort schoot en verklaarde de gehele implementatieregeling ongrondwettig en nietig.

10. Het Ierse hooggerechtshof en het Oostenrijkse grondwettelijk hof werden eveneens geconfronteerd met vragen over de verenigbaarheid van de implementatieregelgeving met privacyrechten. Zij besloten echter, in tegenstelling tot de hoven uit andere lidstaten, een vraag bij het HvJ EU neer te leggen over de verenigbaarheid van de richtlijn als zodanig met de fundamentele rechten zoals die worden gewaarborgd door het Handvest. Het Ierse hooggerechtshof (zaak C-293/12) deed het verzoek in een geding tussen Digital Rights Ireland Ltd. en Ierse overheidsorganen dat de wettigheid betreft van de nationale wettelijke en bestuursrechtelijke bepalingen inzake de bewaring van elektronische communicatie gegevens. Het tweede verzoek, dat van het Oostenrijkse grondwettelijk hof (zaak C-594/12), is ingediend in het kader van de constitutionele beroepen die de regering van het Land Karinthië, Seitlinger en Tschohl en 11.128 andere verzoekers bij de rechterlijke instantie hebben ingesteld. Ook hier gaat het om de verenigbaarheid (van de nationale omzetting) van Richtlijn 2006/24/EC met fundamentele rechten.

11. De centrale vraag die in deze uitspraak wordt beantwoord is die of de Dataretentierichtlijn 2006/24/EG verenigbaar is met de artikelen 7, 8 en 11 van het Hv EU en artikel 8 EVRM. Deze vraag beantwoordt het HvJ EU negatief. De uitspraak is daarbij van grote invloed voor het EU-recht en het recht van de lidstaten, nu het Hof oordeelt over de materiële normen die ten grondslag liggen aan het grootschalig verzamelen van metadata van burgers waartegen geen verdenking bestaat, alsmede de

verplichtingen van de EU-wetgever met betrekking tot het waarborgen van de rechten die zijn neergelegd in het EU-Grondrechtenhandvest.

12. Voor de vaststelling of sprake is van een inmenging verwijst het HvJ naar de conclusie van de A-G. De A-G had gesteld dat het verzamelen en – in het bijzonder – het in een databank bewaren van grote sets metadata van en over de dagelijkse elektronische communicatie van EU-burgers, een ernstige inmenging vormt in het privacyrecht van deze burgers. De gegevensverzameling, zo vervolgde de A-G, creëert de voorwaarden voor surveillance, die gedurende de gehele bewaartermijn en ongeacht of de gegevens worden opgevraagd, een permanente bedreiging vormt voor de privacy. In art. 3 en 6 van de Dataretentierichtlijn worden aanbieders van openbare elektronische communicatiediensten en -netwerken verplicht tot het voor een bepaalde termijn bewaren van gegevens betreffende het privéleven en de communicatie van de gebruikers. Het Hof stemt ermee in dat het stellen van deze verplichting een inmenging oplevert in het recht op eerbiediging van het privéleven en de communicatie (punt 34). Daarnaast vormt de toegang van de bevoegde instanties in de lidstaten tot die gegevens een verdere inmenging in dit recht (punt 35). Het feit dat de gegevens worden bewaard en later worden gebruikt zonder dat de abonnee of de geregistreerde gebruiker hierover wordt ingelicht, kan bij de betrokken personen het gevoel opwekken dat hun privéleven onder constant toezicht staat (punt 37). Het Hof beoordeelt de reikwijdte van de inmenging als zeer ruim en het gewicht ervan als bijzonder zwaar.

13. Het Hof bevestigt verder zijn interpretatie uit de *Österreichischer Rundfunk* (HvJ EU 20 mei 2003, gev. zaken C-465/00, C-138/01 en C-139/01, punt 75), namelijk dat het, om van een inmenging in het privacyrecht te kunnen spreken, niet noodzakelijk is dat de verwerkte gegevens binnen een bijzondere categorie vallen ex art. 8 van de Gegevensbeschermingsrichtlijn (zie punt 33). Ook is het niet noodzakelijk dat de betrokkene schade heeft ondervonden van de verwerking van zijn of haar gegevens. De ondergeschiktheid van deze aspecten is van grote betekenis voor de toetsing van de legitimiteit van surveillancepraktijken, omdat in veel gevallen de effecten van deze programma's niet direct aantoonbaar zullen zijn voor de betrokkenen. Duidelijk is nu dat die moeilijke bewijslast ook inderdaad niet op de betrokkenen rust.

14. Met deze uitspraak weekt het Hof het concept 'vertrouwelijkheid' los van het communicatiegeheim en stelt dit centraal in het recht op eerbiediging van het privéleven. Hierdoor wordt het modern gebruik van alom vertegenwoordigde ICT-systemen en cloud computing onder de beschermingsomvang van artikel 7 Hv gewaarborgd. De A-G gebruikte bij de vaststelling van (de aard van) de inmenging de term 'vertrouwelijkheid van de persoonlijke levenssfeer', als afgeleide van het recht op de eerbiediging van het privéleven (conclusie A-G, hier niet opgenomen, punten 65 en 72). Het HvJ EU bewijst met de verwijzing naar het recht op de vertrouwelijkheid van de persoonlijke levenssfeer een grote dienst aan de EU-burger door, in navolging van het Duitse Bundesverfassungsgericht, de beschermingsomvang van fundamentele rechten te duiden in termen die aansluiten bij de moderne technische architectuur (punt 37; zie eerder Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07; zie in dit verband ook: P. De Hert e.a., 'Duitse rechtspraak over remote searches, datamining en afluisteren op afstand. Het arrest Bundesverfassungsgericht 27 februari 2008 (Online-Durchsuchung) in breder perspectief', *Computerrecht* 2009 (5), p. 200-211; zie ook E.J. Koops, 'Should ICT Regulation be Technology-Neutral?', in: E.J. Koops, M. Lips, C. Prins & M. Schellekens (red.), *Starting Points for ICT regulation Deconstructing prevalent Policy One-Liners* (Vol. 9), Den Haag: T.M.C. Asser Press 2006, p. 77-108).

15. Hoewel het HvJ in zijn eerdere Dataretentie-uitspraak uit 2009 (reeds aangehaald) het verschil benadrukte tussen het bewaren van en de toegang tot metadata en dit laatste

als een nationale aangelegenheid beschouwde, oordeelt het Hof dit keer wel over de evenredigheid van zowel het bewaren als de toegang en daarmee over de inhoudelijke verenigbaarheid van de dataretentie met de fundamentele rechten. Zodra de EU-wetgever de rechten uit het Handvest beperkt is het immers aan diezelfde wetgever om de evenredigheid van die beperkingen te waarborgen.

16. Het Hof overweegt dat dataretentie niet per se een onevenredig middel in de strijd tegen de georganiseerde misdaad hoeft te zijn. De richtlijn is echter vanwege een te algemeen karakter in strijd met het evenredigheidsbeginsel omdat er onvoldoende waarborgen zijn geboden om de inmenging te beperken tot het strikt noodzakelijke. De richtlijn specificeert onvoldoende de omstandigheden waaronder toegang tot de opgeslagen gegevens kan worden verschaft. Ook zijn de bewaartermijnen niet voldoende gemotiveerd en biedt de richtlijn te weinig waarborgen tegen misbruik en onrechtmatige toegang. Daarnaast acht het Hof het verwerpelijk dat in de richtlijn niet wordt geëist dat de opgeslagen gegevens binnen de jurisdictie van de unie worden verwerkt.

17. Het HvJ verklaart om al deze redenen de Richtlijn nietig, wat betekent dat de juridische situatie gelijk is aan die van vóór maart 2006: er rust geen verplichting op de lidstaten om nationale regelingen aan te nemen waarbij aan aanbieders van elektronische communicatiediensten of een openbaar communicatienetwerk verplichtingen worden opgelegd tot het bewaren van metadata voor het garanderen van beschikbaarheid voor onderzoek, opsporing en vervolging van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten.

18. Dit betekent niet dat de maatregelen die op nationaal niveau zijn getroffen, nu ook meteen ongeldig zijn. Het staat de lidstaten immers vrij een “nationale bewaarplicht” te introduceren en wetgevingsmaatregelen treffen om gegevens gedurende een bepaalde periode te bewaren. Dergelijke maatregelen zullen de aanbieders gebieden om te handelen in afwijking van de artikelen 5, 6 en 9 van Richtlijn 2002/58/EG (de e-Privacyrichtlijn), waardoor ze aan de voorwaarden moeten voldoen van art. 15 e-Privacyrichtlijn jo. art. 13 van Richtlijn 95/46/EG (de Gegevensbeschermingsrichtlijn). Wetgeving die het vertrouwelijk karakter van communicatie, verkeersgegevens en andere locatiegegevens binnen een openbaar telecommunicatienetwerk of -dienst (art. 5, 6 en 9 e-Privacyrichtlijn) beperkt, is slechts toelaatbaar indien deze in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van onder andere de staatsveiligheid, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten als bedoeld in art. 13, lid 1 Gegevensbeschermingsrichtlijn. De maatregelen dienen bovendien in overeenstemming te zijn met de algemene beginselen van het Unierecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie, dat naar het EU-Grondrechtenhandvest verwijst (zie art. 15 e-Privacyrichtlijn).

19. Het Handvest is van toepassing op de handelingen van de lidstaten, ‘uitsluitend wanneer zij het recht van de Unie ten uitvoer brengen’ (artikel 51 lid 1 Hv EU). Nu de nationale bewaarplichtwetgeving uitvoering geeft aan uitzonderingen op de EU-regelgeving rondom vertrouwelijkheid van telecommunicatie (e-Privacyrichtlijn), kan worden aangenomen dat het Handvest, ook zonder geldige Dataretentierichtlijn als grondslag, op de nationale wetgeving over de bewaarplicht van toepassing is. Dit betekent dat de nationale regelgeving, hoewel dus niet zonder meer ongeldig, wel verenigbaar moet zijn met dezelfde bepalingen als waaraan het HvJ de Datarichtlijn heeft getoetst. Daarbij kunnen in algemene zin dus ook vergelijkbare eisen worden gesteld.

20. In Nederland is de richtlijn geïmplementeerd in de Wet bewaarplicht, waarbij er voor een bewaartermijn van 6 maanden is gekozen voor internetmetadata en 12 maanden voor telefoniemetadata (Wet van 18 juli 2009 tot wijziging van de Telecommunicatiewet

en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG; zie ook art. 13.2-13.10 Telecommunicatiewet). De interessante vraag is nu uiteraard of de Nederlandse wetgeving de toetsing aan de Handvestbepalingen zou kunnen doorstaan.

21. Allereerst is daarbij van belang dat het HvJ EU juist het alles en ieder treffende karakter van de richtlijn afkeurde, terwijl dit karakter ook in de Nederlandse Wet bewaarplicht is terug te vinden. De Wet bewaarplicht strekt zich, net als de richtlijn, uit tot alle elektronische communicatiemiddelen, die een steeds belangrijker plaats innemen in het dagelijkse leven van de mensen. Bovendien ziet de Nederlandse bewaarplicht, ex art. 13.2a jo. Art. 1.1 onder p en n Telecommunicatiewet, net als de richtlijn op alle abonnees en geregistreerde gebruikers. De maatregel leidt dus tot inmenging in de fundamentele rechten van vrijwel de gehele Nederlandse bevolking. De Wet bewaarplicht besteedt bovendien net zomin als de richtlijn aandacht aan de gebruikswaarde van de gegevens in relatie tot een bepaalde periode, locatie of netwerk van verdachte personen of groep personen die op de een of andere manier kunnen bijdragen aan de strijd tegen ernstige criminaliteit. Op deze punten is de Wet bewaarplicht dus bijzonder kwetsbaar.

22. Daarnaast ontbeert de Wet bewaarplicht, net als de richtlijn, een bepaling die de toegang tot de gegevens verplicht onderhevig maakt aan voorafgaande onafhankelijke toetsing om toegang en gebruik van de metadata te beperken tot het strikt noodzakelijke. Voor het vorderen van verkeersgegevens in Nederland is een vordering van de Officier van Justitie benodigd (art. 126n en 126u Wetboek van Strafvordering). Het Europees Hof voor de Rechten van de Mens bepaalde in 2010 in een zaak tegen Nederland al dat een Officier van Justitie vanwege zijn leidende taak in het strafvorderlijk onderzoek geen onafhankelijke en onpartijdige positie heeft (*Sanoma t. Nederland*, EHRM 14 september 2010, nr. 38224/03, «EHRC» 2010/136 m.nt. Korthals Altes, *NJ* 2011, 230 m.nt. Dommering en Schalken, NbSr 2011, 63, RvdW 2011, 1030, punt. 93). Ook dit maakt dat de Wet bewaarplicht in haar huidige vorm in strijd lijkt te zijn het evenredigheidsbeginsel van artikel 7 en 8 Hv, zoals uitgelegd door het HvJ in *Digital Rights Ireland*.

23. Staatssecretaris Teeven heeft aangegeven de effecten van de uitspraak op de Wet bewaarplicht te onderzoeken (*Handelingen II*, 2013/14, 72, p. 2); ten tijde van schrijven van deze annotatie waren zijn bevindingen nog niet bekend. Ondertussen heeft kamerlid Van Tongeren wel al een initiatiefvoorstel ingediend tot intrekking van de Wet bewaarplicht telecommunicatiegegevens (*Kamerstukken II* 2013/14, 33 939, nr. 1-3). Bij de behandeling van het wetsvoorstel ter invoering van de Wet bewaarplicht in de eerste kamer deelde senator Franken van het CDA mede “politieke opportuniteit” zwaarder te laten wegen dan “wetenschappelijke rationaliteit”, om vervolgens in te stemmen met invoering van de wet (Handelingen I, 2008/2009, nr. 39). Het is interessant te bezien, nu deze uitspraak er ligt, welke van de twee zal prevaleren bij de behandeling van het voorstel tot intrekking van de bewaarplicht.

24. Deze uitspraak van het Hof laat zien dat de catalogus fundamentele rechten de technologische ontwikkeling volgt. De inmenging in deze rechten volgt deze ontwikkelingen echter ook. We moeten een periode afsluiten waarin wetenschappers in de veronderstelling mochten zijn dat “daadwerkelijk inmenging” in de vertrouwelijkheid van communicatie en gegevens simpelweg niet mogelijk was wanneer er gebruik werd gemaakt van versleuteling en wiskundige formules in communicatieprotocollen (zie bijv. R.J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems,* Hoboken: Wiley 2010). De gelekte documenten van klokkenluider Snowden laten echter zien dat - waarschijnlijk onder invloed van geheime diensten -

wetenschappelijke versleutelingsstandaarden worden gemanipuleerd (zie bijv. het project 'BullRun' van de NSA en project 'Edgehill' van de Britse Government Communications Headquarters (GCHQ):
http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide en http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=1&_r=1; voor een wetenschappelijke analyse van één van de (vermoedelijk door geheime diensten) gemanipuleerde standaarden, zie http://projectbullrun.org/dual-ec/index.html, laatstelijk geraadpleegd op 10 juni 2014). De technologische ontwikkeling lijkt in die gevallen te zijn ingegeven door de wens tot inmenging in de vertrouwelijkheid van het privéleven en de communicatie. Het is aan de juristen en computerwetenschappers om beide en in gezamenlijkheid wetenschappelijk rationele keuzes te maken en met systemen te komen die een effectieve bescherming bieden van fundamentele rechten in dit vernieuwde landschap.

M.E. Koning L.L.M., Privacy & Identity Lab, Radboud Universiteit Nijmegen.