Hof van Justitie EU (Grote Kamer)
21 December 2016, zaak C-203/15 en C-698/15
(Lenaerts (President), Tizzano (Vice-President), Silva de Lapuerta, von Danwitz (Rapporteur), da Cruz Vilaça, Juhász en Vilaras. Presidenten van de Kamer Borg Barthet, Malenovský, Levits, Bonichot, Arabadjiev, Rodin, Biltgen en Lycourgos)
Noot: M.E. Koning

**Eerbiediging privéleven en communicatie. Bescherming persoonsgegevens. Vrijheid van meningsuiting. Vertrouwelijkheid van communicatie. Bewaarplicht telecommunicatiegegevens. Wet bewaarplicht. Nationale implementatie EU recht uitzonderingen. Verhouding Handvest en EVRM.**

[art. 5, 6, 9, 15 2002/58EG; art. 13, 22 95/46/EG; art. 7, 8, 11, 52 Hv; 2006/24/EG; art. 13.2 Tw; Wiv]

*In 2014 heeft Tele2 Sverige officieel kennis gegeven van het feit dat zij naar aanleiding van de uitspraak van het HvJ in Digital Rights Ireland de relevante elektronische communicatiegegevens niet meer zou bewaren en de tot dan toe bewaarde gegevens zou vernietigen. Daarover is vervolgens door de nationale politie een klacht ingediend, die is onderzocht door een speciale rapporteur, die daarbij ook heeft gekeken naar de verenigbaarheid van de nationale regeling met de bepalingen waaraan in de uitspraak werd getoetst. Volgens het rapport dat daaruit voortkwam was nader onderzoek naar de regeling nodig. Daarop heeft Tele2 Sverige te horen gekregen dat haar weigering om de gegevens te bewaren in strijd was met de geldende regelgeving en dat zij dit alsnog zou moeten overgaan tot bewaring. Daarover heeft Tele2 vervolgens geprocedeerd en in dat verband zijn prejudiciële vragen gesteld aan het HvJ. In de gevoegde zaak zijn in een Britse zaak aanpalende vragen voorgelegd. In de Britse zaak speelde de reikwijdte van het Europese recht een rol. Het HvJ stelt allereerst vast dat een maatregel als in beide zaken in het geding is, en die aan telecommunicatiedienstenaanbieders de verplichting oplegt om de verkeersgegevens en de locatiegegevens te bewaren, binnen de werkingssfeer van de richtlijn valt, omdat het aanbieden van deze diensten noodzakelijkerwijze inhoudt dat de aanbieders persoonsgegevens verwerken. Bij de beantwoording van de eerste vraag in de Zweedse zaak legt het HvJ uit dat het beginsel van vertrouwelijkheid van communicaties van groot belang is, en afwijkingsmogelijkheden daarvan moeten, gelet op doelstellingen en systeem van de regelgeving, strikt moeten worden uitgelegd. De opsomming van doelstellingen ter doorbreking daarvan is limitatief en het is niet toegelaten om de gegevens voor een ander doel te gebruiken dan is genoemd in art. 15 e-privacy richtlijn en art. 13 Gegevensbeschermingsrichtlijn. Bovendien moeten de bepalingen in het licht van de grondrechten worden uitgelegd. In het bijzonder art. 7 en 8 Hv zijn daarbij van belang, maar ook art. 11 Hv. Dat laatste grondrecht heeft een groot belang in een democratische samenleving. Dit grondrecht is namelijk een van de wezenlijke grondslagen van een democratische en pluralistische samenleving, en behoort tot de waarden waarop de Unie overeenkomstig artikel 2 VEU is gebaseerd. Op grond van art. 52 lid 1 zijn afwijkingen daarvan alleen aanvaardbaar als ze aan de genoemde eisen voldoen, waarbij ze onder meer moeten blijven binnen de grenzen van het strikt noodzakelijke. De Zweedse regeling voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers*

*betreffende alle elektronische communicatiemiddelen, en de aanbieders van elektronische communicatiediensten verplicht deze gegevens stelselmatig en voortdurend te bewaren, zonder enige uitzondering. Daarmee volgt de regeling zeer nauwkeurig de bepalingen uit de ongeldig verklaarde Richtlijn 2006/24/EG. Een dergelijke regeling heeft dezelfde mate van impact als die richtlijn zelf, zoals het HvJ markeert door de relevante passages uit Digital Rights Ireland te herhalen. Een nationale regeling als aan de orde in het hoofdgeding gaat daarmee verder dan strikt noodzakelijk is, en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is. Artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, staat daarentegen niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan de verkeersgegevens en de locatiegegevens ter bestrijding van zware criminaliteit preventief gericht kunnen worden bewaard. Hierbij geldt wel de voorwaarde dat de bewaring van die gegevens, wat de categorieën van te bewaren gegevens betreft, de betrokken communicatiemiddelen, personen en duur van de bewaring, tot het strikt noodzakelijke wordt beperkt. Het Hof somt vervolgens een aantal eisen en voorwaarden op waaraan zo'n nationale regeling dan moet voldoen wat betreft reikwijdte en toepassingsmogelijkheden, waarborgen die ervoor zorgen dat de regeling tot het strikt noodzakelijke wordt beperkt, en objectiviteit van de definitie van de groepen personen waarop de regeling kan worden toegepast.*

*De tweede vraag van de Zweedse rechter ziet op de omvang van de controle op de toegang tot de gegevens door een onafhankelijke bestuurlijke autoriteit of een rechter. In antwoord op deze vraag herhaalt het Hof eerst ook weer de algemene waarborgen die een nationale regeling moet bieden. Vervolgens overweegt het dat het van wezenlijk belang is dat de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens in beginsel, behalve in gevallen van naar behoren gerechtvaardigde spoedeisendheid, wordt onderworpen aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft op een met redenen omkleed verzoek van deze autoriteiten dat met name is ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. Verder is het van belang dat de bevoegde nationale autoriteiten waaraan toegang tot de bewaarde gegevens is verleend, in het kader van de toepasselijke nationale procedures de betrokken personen daarvan op de hoogte brengen wanneer zulks de door deze autoriteiten gevoerde onderzoeken niet in gevaar kan brengen. Het Hof concludeert dat het aan de verwijzende rechterlijke instanties is om na te gaan of en in welke mate de in het hoofdgeding aan de orde zijnde nationale regelingen, zowel ter zake van de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens als ter zake van de bescherming en het niveau van beveiliging van deze gegevens, voldoen aan de eisen die voortvloeien uit artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest.*

*De Britse rechter had ook nog gevraagd of het Hof Digital Rights de artikelen 7 en/of 8 Hv heeft uitgelegd in een zin die verder gaat dan de uitlegging die het EHRM aan artikel 8 EVRM heeft gegeven. Daarbij herhaalt het Hof dat zolang de EU geen partij is bij het EVRM, het geen formeel in de rechtsorde van de Unie opgenomen rechtsinstrument is. De in het onderhavige geval aan de orde zijnde richtlijn 2002/58 moet dus uitsluitend tegen de achtergrond van de door het Handvest gewaarborgde grondrechten worden uitgelegd. Weliswaar moet er de nodige samenhang zijn op*

*grond van art. 52 lid 3, maar van art. 8 Hv is er geen parallel in het EVRM. Een antwoord op de vraag of er meer bescherming wordt verleend door art. 7 en 8 Hv dan door art. 8 EVRM kan daarmee geen invloed hebben op de uitleg van Rl 2002/59; de vraag is daarmee niet-ontvankelijk.*

*Tele2 Sverige AB* (C-203/15)
tegen
*Post- och telestyrelsen,*

en

*Secretary of State for the Home Department (C-698/15)*
tegen
*Tom Watson, Peter Brice, Geoffrey Lewis*

**NOOT**

1.Beleidsmakers en wetgevers trachten nog altijd privacybezwaren omtrent metadata weg te wuiven met een beroep op het geringe belang en de onbeduidendheid van hen die aan de maatregel worden onderworpen, want 'de overheid is echt niet geïnteresseerd in de inhoud van gesprekken'. Wanneer iemand hier commentaar op heeft is er steevast een ander in zijn of haar omgeving die de inperking van privacy wegwuift met een beroep op het geweten, want 'je hebt toch niets te verbergen?'. Gelukkig kijkt het HvJ verder dan deze primaire reacties en benadert het privacy steeds vaker vanuit een maatschappelijk perspectief waarbij de lange termijn gevolgen van zelfcensuur als gevolg van surveillance en de daadwerkelijk waarde van metadata worden meegenomen in de afwegingen. Dit demonstreert het HvJ wederom in de *Tele2*-uitspraak. Na een korte bespreking van de zaak zal ik in deze noot ingaan op de strikte interpretatie van bepalingen door het HvJ, de positionering van profiling en het geografisch criterium dat het HvJ aanhaalt voor een specifieke bewaarplicht. In het laatste deel van deze noot wordt aandacht besteed aan de bredere implicaties van deze uitspraak voor de reikwijdte van het EU-recht en het nationaal veiligheidsrecht.

2. In deze zaak stond de vraag centraal in hoeverre een algemene bewaarplicht voor telecommunicatiegegevens verenigbaar is met het Handvest van de grondrechten EU en welke criteria en waarborgen daarbij zouden moeten gelden. Dit is de derde zaak bij het HvJ over een bewaarplicht van telecommunicatiegegevens (eerder is gewezen *Ierland* t. *Europees Parlement en Raad van de Europese Unie*, HvJ EU 10 februari 2009, zaak C-01/06, «JB» 2009/70 m.nt. Teunissen; *Digital Rights Ireland Ltd* t. *Ierland,* HvJ EU 8 april 2014, gevoegde zaken C-293/12 en C-594/12 «EHRC» 2014/140 m.nt. Koning). *Digital Rights Ireland* ging over de Richtlijn bewaarplicht telecommunicatiegegevens waarin de Europese wetgever het recht op vertrouwelijkheid van communicatie, zoals onderstreept in art. 5 van de e-privacy richtlijn en verankerd in art. 7 en 8 Hv, had beperkt door de lidstaten te verplichten tot het invoeren van bewaarplicht voor telecommunicatiegegevens ten behoeve van de opsporing. (Zie Richtlijn 2006/24/EG, 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). Het

HvJ heeft deze Richtlijn acht jaar na invoering ongeldig verklaard en vernietigd, omdat de Europese wetgever de door het evenredigheidsbeginsel gestelde grenzen had overschreden die hij in acht dient te nemen in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest.

3. De lidstaten bleven achter met een nationale regeling die in veel gevallen grote gelijkenissen vertoonde met de inhoud van de buiten werking gestelde Richtlijn bewaarplicht telecommunicatiegegevens. In Nederland was de richtlijn bijvoorbeeld opgenomen in de Wet bewaarplicht telecommunicatiegegevens (wet van 1 september 2009, *Stb*. 2009, 333). Na toetsing aan de criteria van de *Digital Rights Ireland*-zaak stelde de Haagse voorzieningenrechter in maart 2015 de Wet bewaarplicht buiten werking wegens strijdigheid met het evenredigheidsbeginsel. (Rb. Den Haag 11 Maart 2015, ECLI:NL:RBDHA:2015:2498, Computerrecht 2015/88, m.nt. van der Jagt) De Nederlandse wetgever ging daarna terug naar de tekentafel en volgde met een voorstel voor een herziende wettelijke regeling voor het verplicht bewaren van telecommunicatiegegevens (TK 2016–2017, Kamerstuk 34 537, nr. 2). De inkt van dit voorstel was nog niet droog of de wetgevingsjuristen moeten alweer terug naar de tekentafel om de *Tele2*-zaak te bestuderen en de hernieuwde bewaarplicht in lijn te brengen met de eisen van deze uitspraak. Ten tijde van het schrijven van deze noot zijn de resultaten van dit laatste werk nog niet bekend (TK 2016–2017 Kamerstuk 34 537, nr. 6). Toch kan met enige zekerheid worden gezegd dat het voorstel zoals dit er nu ligt (TK 2016–2017, Kamerstuk 34 537, nr. 2) in strijd is het de fundamentele rechten uit het Handvest omdat na de *Digital Rights Ireland*-zaak de Nederlandse wetgever nog steeds lijkt uit te gaan van de legitimiteit van een algemene bewaarplicht. De concrete handvatten die het HvJ in de *Tele2*-uitspraak meegeeft zijn: een verbod op een algemene bewaarplicht. In geval van een specifieke bewaarplicht eist het HvJ dat de toegang tot gegevens beperkt blijft tot het doel van bestrijding van ernstige criminaliteit, dat die toegang aan een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit is onderworpen, en dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard (punt 125).

4. Hamerend op de positie van uitzondering die een beperkende maatregel moet blijven voor de rechten uit het Handvest, zet het HvJ een streep door een algemene generieke bewaarplicht omdat een dergelijke regeling de grenzen van het strikt noodzakelijke overschrijdt (punt 107). Het HvJ legt uit dat de mogelijkheid tot inperking van het recht op vertrouwelijkheid van communicatie, zoals omschreven in artikel 15 e-privacy richtlijn (en *inter alia* art. 13 Gegevensbeschermingsrichtlijn) niet zo ver rijkt dat deze een nationale algemene bewaarplicht telecommunicatiegegevens kan omvatten. In de uitspraak zet het HvJ drie striktheidsvereisten uiteen waaraan een regeling die is gebaseerd uit art. 13 Gegevensbeschermingsrichtlijn of art. 15 e-privacy richtlijn moet voldoen. Ten eerste herinnert het HvJ er aan dat beperkingen op het onderliggende fundamenteel recht tot eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens (art. 7 en 8 Hv) alleen zijn toegestaan voor zover deze strikt noodzakelijk zijn (punt 96). Ten tweede gaat het om een uitzondering die niet de regel mag worden. Het HvJ achtte de Zweedse en Britse bewaarplicht te ruim omdat de locatie- en verkeersgegevens standaard van iedere aansluiting werden bewaard voor het doel van opsporing (punt 104). Tot slot stipuleert het HvJ in lijn met eerdere uitspraken dat de doelen waarvoor fundamentele

rechten mogen worden beperkt uitputtend zijn genoemd in art. 13 Gegevensbeschermingsrichtlijn of art. 15 e-privacy richtlijn (punten 90, 102 en 115).

5. Haarfijn legt het HvJ de mogelijkheden uit van profilering met metadata ofwel 'gegevens over gegevens' – bijvoorbeeld wie belt met wie, waar en wanneer. Het HvJ erkent dat uit deze gegevens zeer precieze conclusies kunnen worden getrokken over het privéleven van personen, zoals hun dagelijkse gewoonten, permanente of tijdelijke verblijfplaats, dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren (punt 99). Vervolgens concludeert het HvJ dat de informatie die zo'n profiel prijs geeft, wat betreft het recht op bescherming van het privéleven, gevoelig is – net als de inhoud van gesprekken (punt 99). Het HvJ is echter niet van mening dat het bewaren van metadata de essentie schaadt van het recht op eerbiediging van het privéleven bij de verwerking van persoonsgegevens (art. 7 en 8 Hv), maar een bewaarplicht kan wel invloed hebben op het gebruik van de elektronische communicatiemiddelen en dus op de wijze waarop iemand van de vrijheid van meningsuiting gebruikmaakt, ex art. 11 Hv (punt 101). Het HvJ tilt hier zwaar aan en verbindt op deze manier de uitingsvrijheid en het gevaar van zelfcensuur aan intellectuele privacy, waardoor aan dat laatste recht een anno 2017 noodzakelijke maatschappelijke betekenis wordt toegekend. (Zie over dit onderwerp ook: N. Richards, *Intellectual privacy: Rethinking civil liberties in the digital age*, Oxford: Oxford University Press, 2014.)

6. Het HvJ stelt vervolgens vast dat de tekst van art. 15 e-privacyrichtlijn wel de mogelijkheid geeft voor een specifieke bewaarplicht en om deze reden onderstreept het HvJ een aantal minimale criteria waar een dergelijke specifieke regeling aan moet voldoen (punten 114-123). Zo legt het HvJ uit dat een specifieke bewaarplicht enkel mag worden ingezet ter bestrijding van ernstige criminaliteit. De bewaring moet dan ook op dit doel zijn toegespitst waarbij een verband bestaat tussen doel, bewaarcriteria en de opgeslagen gegevens (punt 119). De afbakening ter zake van de personen en situaties die onder de maatregel vallen, kan volgens het HvJ geschieden langs geografische en groepslijnen – mits objectief toegepast. In de praktijk zal dit neerkomen op de situatie waarbij de bevoegde autoriteiten een bewaarplicht instellen voor een straat, buurt, wijk, stad, gemeente of provincie wanneer een hoog risico bestaat dat ernstige criminaliteit wordt voorbereid of gepleegd. Deze benadering van het HvJ is in mijn ogen niet onproblematisch. Zo zal de afbakening van een te groot gebied op dezelfde bezwaren stuiten als een generieke bewaarplicht: de regeling is niet beperkt tot het strikt noodzakelijke. De redenering die het HvJ in punt 105 van de uitspraak neerlegt voor een generieke algemene bewaarplicht zal in het geval van een groot gebied ook opgaan voor een specifieke bewaarplicht. De afbakening van een kleiner geografisch gebied kan spanning op leveren met het verbod op discriminatie (art. 14 EVRM) omdat mensen die tot een bepaalde groep behoren geregeld in hetzelfde gebied wonen, zeker als het om minderheden gaat. Beleid op grond van een postcodereeks vertaalt zich maar al te snel naar ongelijke behandeling omdat indirect onderscheid wordt gemaakt op grond van ras, kleur, taal, godsdienst, nationale of maatschappelijke afkomst, het behoren tot een nationale minderheid en/of vermogen. Het is jammer dat het HvJ deze spanning niet opmerkt en handvatten meegeeft voor het opstellen van het toekomstig beleid.

7. Het laatste punt dat ik bespreek in deze noot is die van de werkingssfeer van het EU gegevensbeschermingsrecht en daarmee verbandhoudend het Handvest. Door het

HvJ wordt dit behandeld in de punten 62 tot en met 81. Het HvJ werkt een redenering uit die gevolgen zal hebben voor de afbakening van grondrechten in het nationaal veiligheidsdomein en de soevereiniteit van lidstaten als het gaat om gegevensstromen van particuliere gegevensverwerkers naar inlichtingen- en veiligheidsdiensten. Ten tijde van het schrijven van deze noot is dit een bijzonder relevant onderwerp in Nederland omdat de Wet op de inlichtingen- en veiligheidsdiensten wordt herzien. Het HvJ beklemtoont in punt 73 dat vanuit Europees perspectief rechtbeperkende nationale regelingen onder de reikwijde van het EU recht vallen. Het Luxemburgs Hof past een teleologische interpretatie toe wanneer het de werkingssfeer uitlegt van de e-privacy richtlijn en de Gegevensbeschermingsrichtlijn. Artikel 1, derde lid, e-privacy richtlijn en *inter alia* art. 3, tweede lid, Gegevensverwerkingsrichtlijn sluiten werking van de twee richtlijnen uit voor de activiteiten van *de Staat* op een aantal gebieden, waaronder de openbare veiligheid, defensie en de staatsveiligheid (punt 69). De activiteiten *van particulieren* op deze gebieden rekent het HvJ echter wel tot de werkingssfeer van het Europees recht (punten 69 en 72). Dit laatste is niet meteen helder uit de preambule of de tekst van de betreffende richtlijnen, maar blijkt wel uit de opbouw van deze instrumenten. In beide gevallen wordt na bepaling van de reikwijdte een aantal rechten voor de betrokkene en plichten voor de gegevensverwerker gestipuleerd. De reikwijdte van die rechten en plichten kunnen op hun beurt worden beperkt onder strikte voorwaarden voor een beperkt aantal doelen, waaronder de openbare veiligheid, landsverdediging en de veiligheid van de Staat, ex art. 15 e-privacy richtlijn en art. 13 Gegevensbeschermingsrichtlijn (zie in dit verband ook randnr. 4 van deze noot). Het HvJ merkt terecht op dat wanneer dit anders zou zijn elk nuttig effect wordt ontnomen aan art. 15 e-privacy richtlijn en *inter alia* art. 13 Gegevensbeschermingsrichtlijn (punt 73). Daarnaast dienen beide bepalingen gelezen te worden in het licht van de grondrechten uit het Handvest (punt 91 en de aldaar genoemde jurisprudentie). Volgens artikel 52, eerste lid, Hv moeten beperkingen op de grondrechten bij wet worden gesteld en de wezenlijke inhoud daarvan eerbiedigen. Omdat het evenredigheidsbeginsel in acht moet worden genomen, kunnen slechts beperkingen worden gesteld die noodzakelijk zijn en daadwerkelijk beantwoorden aan door de EU erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen (punt 94).

8. Het voorgaande onderstreept twee dingen voor gegevensstromen van particuliere gevensverwerkers naar inlichtingen- en veiligheidsdiensten. Ten eerste valt de gegevensverwerking aan de zijde van de particuliere verwerker onder het EU recht. Ten tweede moet de beperkende nationale regeling voldoen aan de voorwaarden uit art. 15 e-privacy richtlijn en/of art. 13 Gegevensbeschermingsrichtlijn en art. 7, 8, 11 en 52, eerste lid, Hv. Maar hoe vertaalt deze redenering zich naar de praktijk van nationale veiligheid? Gegevensstromen van particuliere gevensverwerkers naar inlichtingen- en veiligheidsdiensten roepen de onverbiddelijke vraag op waar de particuliere gegevensverwerking ten behoeve van de openbare veiligheid, landsverdediging en de veiligheid van de Staat stopt en de staatsactiviteiten op deze terreinen beginnen. Een vraag die hiermee verbonden is, betreft welk gedeelte van de beperkende maatregel onder het EU recht valt en welk gedeelte onder het nationale recht valt. Deze vraag is des te prangender nu het om nationaal veiligheidsbeleid gaat, een van oudsher exclusief juridisch domein van de van lidstaten (art. 4, tweede lid, VEU). Het HvJ lijkt hier een antwoord op te geven in de *Tele2*-zaak. In punt 79 oordeelt het HvJ dat met betrekking tot de bewaarplicht de gegevens uitsluitend

langer bewaard bleven om de bevoegde autoriteiten in voorkomend geval toegang te geven tot die gegevens. De nationale regeling die verplicht tot de bewaring van de gegevens bevat in een dergelijk geval ook noodzakelijkerwijs bepalingen betreffende de toegang tot die gegevens, aldus het HvJ. Het HvJ legt de grens van het EU recht en het nationale recht niet langs de hierboven genoemde formele lijnen in de primaire verdragen, maar voert een inhoudelijke toetsing uit waarbij gekeken wordt naar de invloed van de toegang op de verwerking van de gegevens bij de particuliere gegevensverwerker. Wanneer de toegangsprocedure van de diensten tot de gegevens bepalend is voor de verwerking van de gegevens aan de zijde van de partuculier, vallen in een dergelijk geval de toegansprocedures ook onder de reikwijdte van het EU recht. Met deze redenering laat de Unie nationale veiligheid de verantwoordelijkheid van de lidstaten maar stelt zij wel eisen aan regels uit dit domein die de grondrechten uit het Handvest beperken. Vanuit het perspectief van fundamentele rechten is dit een goede ontwikkeling omdat bij de vaststelling van de werkingssfeer van het EU recht de materiële omvang van de richtlijnen en de grondrechten boven de  de soevereiniteitskwesties van de lidstaten en de EU worden gesteld.

9. Deze overwegingen van het HvJ zijn van invloed op de het nationale veiligheidsrecht van de lidstaten. In Nederland is dat vastgelegd in de Wet op de Inlichtingen- en veiligheidsdiensten die momenteel wordt herzien. Als het gaat om verplichte en vrijwillige gegevensverstrekkingen van particuliere gegevensverwerkers aan de diensten, wuift de Nederlandse wetgever – in stijd met de *Tele2*-uitspraak – in algemene termen de verplichtingen weg voor de verwerkingsverantwoordelijke die voortvloeien uit het gegevenbeschermingsrecht (art. 39, vijfde lid, juncto 39, eerste lid,, 52, vierde lid,, 54, vijfde lid,, 55, vijfde lid,, 56, vijfde lid, voorstel voor een Wet op de inlichtingen- en veiligheidsdiensten (Wiv),  TK 2016–2017, Kamerstuk 34 588). Omdat het Europees gegevensbeschermingsrecht de gegevensverwerking aan de zijde van particuliere reguleert heeft dit twee gevolgen. Ten eerste moeten de eerder aangehaalde bepalingen uit de Wiv voldoen aan de eisen van art. 15 e-privacy richtlijn en/of art. 13 Gegevensbeschermingsrichtlijn en art. 7, 8, 11 en 52, eerste lid, Hv. Het Handvest speelt dus in geval van privaat naar publieke gegevensstromen een rol bij de uitvoering van de Wiv. Ten tweede blijven de bepalingen uit de richtlijnen die niet via art. 15 e-privacy richtlijn en/of art. 13 Gegevensbeschermingsrichtlijn mogen worden beperkt, in volledige omvang van toepassing op de gegevensverstrekking. Hieronder vallen onder meer verplichtingen die betrekking hebben op de aansprakelijkheid van de verwerkingsverantwoordelijke in geval van onrechtmatige verwerking en de verplichting tot beveiliging van de gegevens (art. 17 Gegevensbeschermingsrichtlijn). Het in algemene zin niet van toepassing verklaren van de bij of krachtens de wet geldende voorschriften voor de verwerkingsverantwoordelijke op de verstrekkingen aan inlichtingen- en veiligheidsdiensten, zoals in de Wiv wordt voorgesteld, is om bovenstaande redenen in strijd met het Europese recht.

10. Het EU-recht werkt ook door in het nationale veiligheidsdomein middels de toegangsprocedures tot gegevens bij particuliere gegevensverwerkers. Een aantal bepalingen –bijvoorbeeld voor pre-paid simcards – uit het voorstel voor de Wiv zijn gevoelig voor dit soort doorwerking. Art. 56, eerste lid, Wiv verplicht een communicatiedienst tot  verstrekking van gegevens over de identiteit van een gebruiker (personalia). Wanneer een aanbieder van een openbaar

telecommunicatienetwerk of openbare telecommunicatiedienst geen identificerende gegevens van een gebruiker blijkt te hebben kan de dienst in bepaalde gevallen de aanbieder verplichten om deze gegevens te achterhalen en deze aan de dienst te verstrekken, ex art. 56, tweede lid, Wiv. Op dat moment verandert aan de zijde van de aanbieder de verwerking van pseudonieme gegevens in verwerking van identificerende gegevens. De verwerking van personalia en de koppeling met inhoud en metadata van communicatie vindt dan uitsluitend plaats om de diensten de gegevens te verstrekken. De toegang van de diensten tot de gegevens is bepalend voor de identificering, waardoor de toegangsregels deel uitmaken van de beperkende maatregel op het recht op vertrouwelijkheid van communicatie ex art. 5 en 6 e-privacy richtlijn. De toegangsregeling van artikel 56 Wiv moet om deze reden voldoen aan de eisen van artikel 15 e-privacy richtlijn en art. 7, 8, 11 en 52, eerste lid, Hv.

11. Publiek-private samenwerking wordt de toekomst van het nationale veiligheidswezen genoemd, maar juridisch heeft dit nogal wat addertjes onder het gras. In de toekomst zal de grondrechtelijke beschermingsmissie van de EU waarschijnlijk gaan botsen met nationale regels ter bescherming van de nationale veiligheid in geval van gegevensstromen van particuliere gevensverwerkers naar inlichtingen- en veiligheidsdiensten. Ik ben benieuwd of het HvJ in toekomstige gevallen de *Tele2*-argumentatie aanhoudt en de grens van het EU recht en het nationale recht niet trekt langs de formele lijnen uit de primaire verdragen, maar aan de hand van een inhoudelijke toetsing op invloed, toegang en doel van de verwerking van de betrokken partijen.