Massasurveillance en privacy: De betekenis van het EHRM-arrest *Big Brother Watch e.a. t. het Verenigd Koninkrijk* voor het EU-recht

mr. dr. M. Hagens en prof. dr. C.M.J. Ryngaert[1]

1. Inleiding

In 2013 onthulde Edward Snowden het bestaan van een programma (PRISM) waarmee de Amerikaanse *National Security Agency* informatie vergaarde van aanbieders van elektronische communicatiediensten. Uit gelekte documenten bleek dat ook één van de Britse geheime diensten (*Government Communications Headquarters* – GCHQ) toegang had tot PRISM. GCHQ gaf later toe dat het inderdaad informatie had verkregen via PRISM. Edward Snowden onthulde ook dat GCHQ zelf een operatie had opgezet, genaamd 'TEMPORA', waarmee het grote hoeveelheden gegevens aftapte van Internetkabels. Tien mensenrechtenorganisaties, waaronder *Big Brother Watch*, waren van oordeel dat het Verenigd Koninkrijk (VK) hiermee de mensenrechten had geschonden, met name het recht op privacy zoals neergelegd in art. 8 EVRM.

Het Europees Hof voor de Rechten van de Mens (EHRM) gaf hen in een arrest van 13 september 2018 deels gelijk (*Big Brother Watch e.a. t. Verenigd Koninkrijk*).[2] Het EHRM was van oordeel dat het VK bij bulkinterceptie onvoldoende toezicht uitoefende over de keuze welke internetkabels afgetapt zouden worden en over de keuze van selectoren en zoekcriteria om onderschepte communicatie te filteren. Ook vond het EHRM dat er onvoldoende waarborgen waren om te voorkomen dat metadata van inwoners van het VK werden verzameld, en dat rechten van journalisten waren geschonden (art. 10 EVRM). Wat het verkrijgen van door de VS verzamelde gegevens betreft, oordeelde het EHRM dat er voldoende waarborgen bestonden. Hier deed zich geen schending van art. 8 EVRM voor. Er was wel sprake van een schending van art. 8 EVRM bij het opvragen van communicatiegegevens (metadata) van elektronische communicatiediensten omdat het doel van de toegang niet beperkt was tot het bestrijden van 'ernstige misdrijven', en er niet was voorzien in voorafgaand onafhankelijk toezicht.

Hier gaan we niet uitgebreid in op de uitspraak zelf en de betekenis ervan voor de Nederlandse context. Voor een uitgebreide samenvatting en commentaar verwijzen we graag naar de annotatie van Mireille Hagens[3] die de uitspraak bespreekt tegen de achtergrond van eerdere uitspraken van het EHRM, zoals de Zweedse zaak *Rättvisa t. Zweden* over bulkinterceptie,[4] en de totstandkoming van de nieuwe Nederlandse wetgeving voor de inlichtingen- en veiligheidsdiensten (Wiv 2017).[5] In dit artikel belichten

1. Mireille Hagens is senior-onderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) en gastonderzoeker bij het Departement Rechtsgeleerdheid van de Universiteit Utrecht. Deze bijdrage is op persoonlijke titel geschreven. Cedric Ryngaert is hoogleraar internationaal publiekrecht aan de Universiteit Utrecht. Hij is verbonden aan het onderzoeksprogramma RENFORCE (Regulation and Enforcement in Europe) van het Departement Rechtsgeleerdheid (Faculteit REBO). Wat Ryngaert betreft: het onderzoek dat in deze publicatie heeft geresulteerd, werd gefinancierd door de *European Research Council* o.b.v. het *Starting Grant Scheme* (Proposal 336230—UNIJURIS) en door NWO (VIDI Nr. 016.135.322).
2. EHRM 13 september 2018, *Big Brother Watch e.a. t. het Verenigd Koninkrijk*, nrs. 58170/13, 62322/14, 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013.
3. *European Human Rights Cases* (EHRC), combi-annotatie van M. Hagens bij 2018/208 (*Big Brother Watch e.a.*) en 2018/196 (*Rättvisa*).
4. EHRM 19 juni 2018, *Centrum för Rättvisa t. Zweden*, nr. 35252/08, ECLI:CE:ECHR:2018:0619JUD003525208.
5. Zie met name *European Human Rights Cases* (EHRC), combi-annotatie van M. Hagens bij 2018/208 (*Big Brother Watch e.a.*) en 2018/196 (*Rättvisa*), punt 19, waarin zij het volgende stelt: 'Afgaande op het beoordelingskader zoals dit in *Centrum för Rättvisa* door het Hof is herhaald en in *Big Brother Watch e.a.* opnieuw is bevestigd, denk ik dat de Wiv 2017 op het punt van bulk-interceptie in voldoende waarborgen voorziet om de test van artikel 8 EVRM te kunnen doorstaan'. In lijn met deze en eerdere jurisprudentie van het EHRM (zie

wij in de eerste plaats het belang van de zaak *Big Brother Watch e.a.* voor het EU-recht, en vice versa. Eerst bespreken wij de principiële betekenis van de jurisprudentie van het EHRM voor het EU-recht, met name in de context van surveillance (deel 2). Vervolgens gaan we na hoe het EVRM-recht, zoals geïnterpreteerd door het EHRM, zich verhoudt tot het EU-recht ter zake, zoals geïnterpreteerd door het EU-Hof van Justitie (HvJ). Met name trachten we aanwijzingen voor convergentie dan wel divergentie te distilleren uit *Big Brother Watch e.a.* (deel 3). Deel 4 bevat enkele afsluitende opmerkingen.

2. Betekenis van de jurisprudentie van het Europees Hof voor de Rechten van de Mens voor het EU-recht

In algemene zin heeft de EHRM-zaak *Big Brother Watch e.a.* potentiële relevantie voor het EU-recht. De reden is dat het EU-Handvest van de Grondrechten[6] bepaalt dat de inhoud en reikwijdte van de EU-grondrechten dezelfde zijn als die van de EVRM-rechten, tenzij die rechten niet volledig corresponderen.[7] De discussie over de verhouding tussen het EVRM- en het EU-recht is geenszins aca-

Big Brother Watch e.a., par. 320), is de praktijk van de uitvoering van het wettelijk kader van belang bij de beoordeling van een wettelijk systeem voor inlichtingen- en veiligheidsdiensten. Voor de Wiv 2017, die op 1 mei 2018 in werking is getreden, moet de praktijk uitwijzen of de balans in de wet en de waarborgen voldoende zijn. Het toezicht op de AIVD en de MIVD en de aangekondigde (vervroegde) evaluatie van de wet na twee jaar vervullen hierbij een belangrijke rol. De zaak *Big Brother Watch e.a.* betreft nog een ander onderwerp dat in dit artikel niet wordt betrokken, maar dat wel (mede) van belang is voor de Nederlandse context. Het voert te ver om hier op deze plaats uitgebreid op in te gaan. Volstaan wordt met een korte indicatie: Het gaat over samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten en dan met name het delen van gegevens. Dit is de eerste keer dat het EHRM zich hierover uitspreekt, al beperkt de uitspraak zich, gezien de klacht, tot het (op verzoek) ontvangen van gegevens uit het buitenland (niet het verstrekken aan het buitenland). In Nederland heeft over precies dit onderwerp een aantal belangenorganisaties een zaak aangespannen tegen de Nederlandse Staat. Dit vond plaats in de nasleep van de onthullingen van Edward Snowden: Deze organisaties verwijten de Nederlandse inlichtingen- en veiligheidsdiensten dat zij op ongeoorloofde wijze verworven gegevens uit de Verenigde Staten en het Verenigd Koninkrijk ontvangen en daardoor zelf onrechtmatig handelen. Ook stellen zij dat de wettelijke basis voor het ontvangen van gegevens in de Wiv 2002 onvoldoende is. Nog voordat deze procedure door de Hoge Raad was behandeld, kregen de belangenorganisaties toestemming zich als derde partijen te voegen in de gecombineerde zaken *Big Brother Watch e.a.* Net voor het EHRM deed de Hoge Raad uitspraak (HR 7 sept. 2018, *Burgers t. Plasterk*, ECLI:NL:HR:2018:1434): Cassatie werd verworpen, de uitspraak van het gerechtshof werd bevestigd (Gerechtshof 14 maart 2017, ECLI:NL:GHDHA:2017:535). Het ontvangen van gegevens uit het buitenland werd niet verboden. Uitgangspunt hierbij is het vertrouwensbeginsel. De AIVD en de MIVD mogen erop vertrouwen, behoudens concrete aanwijzingen van het tegendeel, dat diensten waarmee wordt samengewerkt hun verplichtingen onder nationale en internationale wet- en regelgeving nakomen (r.o. 3.2.2). Het gerechtshof heeft de vorderingen van eisers juist opgevat, namelijk dat deze alleen gaan over gegevens die op onrechtmatige wijze zijn verkregen, en niet op de ontvangst van gegevens van buitenlandse diensten in het algemeen (r.o. 3.3.3.). De HR vindt ook dat het gerechtshof mocht oordelen dat eisers onvoldoende hebben aangetoond dat de buitenlandse inlichtingendiensten onrechtmatig handelen bij het verkrijgen van inlichtingen. Verder is niet gebleken dat de Nederlandse diensten systematisch of willens en wetens gegevens van buitenlandse inlichtingendiensten zouden ontvangen omtrent Nederlandse burgers, terwijl zij deze gegevens niet op grond van hun eigen bevoegdheden hadden kunnen vergaren (r.o. 3.2.2). De HR vindt van belang dat de relevante wetgeving in de Verenigde Staten sinds de 'Snowden-onthullingen' is veranderd en dat eisers over de gevolgen van die nieuwe wetgeving te weinig hebben gezegd (r.o. 3.4.3). Thans rest nog de weg naar het EHRM. Het EHRM deed na de HR uitspraak in *Big Brother Watch e.a.* op 13 sept. 2018. Het EHRM oordeelt dat de inbreuk ligt in de ontvangst van verzochte gegevens en de daaropvolgende bewaring, onderzoek en gebruik ervan (par. 421), omdat de interceptie ervan door de NSA, zelfs als deze interceptie op verzoek van het VK plaatsvond (ondersteuning), buiten de controle van het VK plaatsvond (par. 420). Dat laat onverlet dat de zes minimumwaarborgen die gelden voor (bulk)interceptieregimes (par. 307/315, zie ook noot 34 in dit artikel) ook op het ontvangen van gegevens van toepassing zijn. Het is van belang dat staten niet hun eigen verplichtingen (en beperkingen) kunnen omzeilen, daarom moet geregeld zijn onder welke omstandigheden een verzoek aan een buitenlandse dienst kan worden gedaan om materiaal te kunnen ontvangen. Daar zit immers het grootste risico (u-bocht) (par. 423-424). Het EHRM overweegt: '*Due to the nature of global terrorism, and in particular the complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a flow of information between the security services of many countries in all parts of the world. As, in the present case, this "information flow" was embedded into a legislative context providing considerable safeguards against abuse, the Court would accept that the resulting interference was kept to that which was "necessary in a democratic society".*' (par. 446). De Wiv 2002 regelde het ontvangen van gegevens (op verzoek) niet expliciet, maar het werd verondersteld te vallen onder de samenwerkingsbepaling van art. 59 Wiv 2002 (ondersteuning) en de algemene vereisten voor gegegevensverwerking in art. 12 Wiv 2002 (CTIVD, toezichtsrapport nr. 38 en juridische bijlage (par. VI.3 en VI.4), www.ctivd.nl). De Wiv 2017 regelt het verzoeken om ondersteuning aan een buitenlandse dienst (bv inzet bijzondere bevoegdheid, zoals bulkinterceptie en het ontvangen van de daaruit verkregen gegevens) in art. 90.

6. Handvest van de grondrechten van de Europese Unie, *Pb. C 326/391* (2012).
7. Art. 52.3 Handvest. Zie ook art. 6.3 EU-verdrag dat bepaalt dat de grondrechten zoals zij worden gewaarborgd door het EVRM als algemene beginselen deel uitmaken van het Unierecht.

demisch in de context van surveillance (geheim onderzoek) en gegevensverzameling. Het HvJ heeft op deze terreinen intussen al verschillende uitspraken gedaan over de verenigbaarheid met de EU-grondrechten van Europese en nationale maatregelen, zoals in *Digital Rights Ireland Ltd en Seitlinger e.a.*[8], *Tele2 Sverige AB en Watson*[9], *Schrems*[10] en *Canada-EU Passenger Names Records*[11]. Het EHRM heeft zich in de afgelopen jaren meermaals uitgesproken over massasurveillance in een strafrechtelijke en nationale veiligheidscontext. Hierbij geldt de zaak *Big Brother Watch e.a.* tot op heden als het sluitstuk. In deze zaak verduidelijkt het EHRM zijn eerdere jurisprudentie, met name over bulkinterceptie en toegang tot gegevens, en plaatst deze in context. Een interessante samenloop met de EU-jurisprudentie doet zich niet alleen op dat terrein voor, maar met name ook bij de toegang van de autoriteiten tot door communicatiediensten opgeslagen gegevens.[12]

De samenloop tussen beide hoven gaat een nieuwe ronde in. Op dit ogenblik is bij het HvJ een Brits verzoek om een prejudiciële beslissing aanhangig over de toepassing van vereisten voor de verwerking van bulkgegevens en geautomatiseerde processen die noodzakelijk zijn om de nationale veiligheid te beschermen *(Privacy International v. Secretary of State*[13]*).* Het daaraan ten grondslag liggende geschil betreft de bevoegdheid van de Britse minister van Binnenlandse Zaken om in het belang van de nationale veiligheid in bulk communicatiegegevens (metadata) op te vragen bij private aanbieders van communicatiediensten, zoals internet- en telecomproviders. De inlichtingen- en veiligheidsdiensten kunnen de gegevens vervolgens ongericht en met behulp van geautomatiseerde data-analyse onderzoeken om ongekende dreigingen te onderkennen. De prejudiciële vraag die hieruit volgt is of het opvragen van metagegevens in het belang van de nationale veiligheid onderworpen is aan de voorwaarden in de E-privacyrichtlijn (2002/58/EG), die het HvJ nader heeft ingevuld in de uitspraak *Tele2 Sverige AB en Watson*.[14] In het geval van een bevestigend antwoord, luidt de volgende prejudiciële vraag of het EU-recht aanvullende eisen stelt bovenop de eisen die voortvloeien uit het EVRM, en vervolgens of de eisen die het HvJ in *Tele2 Sverige AB en Watson* stelt dan op gelijke wijze gelden voor de uitoefening van genoemde bevoegdheid in de nationale veiligheidscontext. Het verzoek betreft een verduidelijking van de uitspraak in *Tele2 Sverige AB en Watson*.[15] Voorafgaand aan deze uitspraak had het HvJ in de gevoegde zaken *Digital Rights Ireland Ltd en Seitlinger e.a.* de Dataretentierichtlijn (2006/24/EG) nietig verklaard wegens strijd met art. 7 en 8 EU-Handvest van de Grondrechten. Deze richtlijn vormde in bijna alle Europese landen de basis voor een algemene en ongedifferentieerde bewaarplicht voor aanbieders van telecommunicatie. Deze bewaarplicht zag erop alle verkeers- en locatiegegevens van alle communicatiemiddelen van alle gebruikers tussen zes maanden en twee jaar te bewaren ten behoeve van de bestrijding van criminaliteit (dataretentie). De daarop volgende uitspraak van het HvJ in de gecombineerde zaken *Tele2 Sverige AB en Watson* ging nader in op de verenigbaarheid van de Zweedse en Engelse bewaarplicht met de E-privacyrichtlijn (2002/58/EG) en het EU-Grondrechtenhandvest. Hierin bepaalde het HvJ dat het Unierecht zich niet verzet tegen 'gerichte' bewaring van metagegevens, mits dit aan een aantal voorwaarden voldoet. Zo mag de bewaring alleen geschieden voor de bestrijding van 'ernstige' criminaliteit en dient tot het strikt noodzakelijke beperkt te zijn. Verder dient de bewaring plaats te vinden op het grondgebied van de Unie en dient de toegang van de nationale autoriteiten tot de bewaarde gegevens aan (strikte) voorwaarden te zijn onderworpen, met name voorafgaande toetsing door een onafhankelijke (gerechtelijke) instantie. De uitspraak biedt weinig handvatten voor de precieze vertaalslag van deze vereisten naar het nationale niveau, met name de invulling en afbakening van de gerichtheid van de bewaring.[16] Ook is onduidelijk of de uitspraak

8. HvJ EU 8 april 2014, *Digital Rights Ireland Ltd* en *Seitlinger e.a.*, C-293/12 en C-594/12, ECLI:EU:C:2014:238.
9. HvJ EU 21 december 2016, *Tele2 Sverige AB* en *Watson*, C-203/15 en C-698/15, ECLI:EU:C:2016:572 en ECLI:EU:C:2016:970.
10. HvJ EU 6 oktober 2015, *Maximilian Schrems t. Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.
11. Hv JEU 26 juli 2017, Advies 1/15 van het Hof (Grote kamer) over de voorgenomen overeenkomst tussen de EU en Canada inzake doorgifte van passagiersgegevens, ECLI:EU:C:2017:592.
12. Zie ook EHRM 4 december 2015 (GK), *Zakharov t. Rusland*, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, *NJ* 2017/185, m.nt. Dommering, *EHRC* 2016/87, m.nt. Hagens; EHRM 8 februari 2018, *Ben Faiza t. Frankrijk*, nr. 31446/12, ECLI:CE:ECHR:2018:0208JUD003144612, *EHRC* 2018/85, m.nt. M. Hagens.
13. C-623/17.
14. HvJEU 21 december 2016, *Tele2 Sverige AB* en *Watson*, C-203/15 en C-698/15, ECLI:EU:C:2016:572 en ECLI:EU:C:2016:970, par. 99.
15. HvJEU 21 december 2016, *Tele2 Sverige AB* en *Watson*, C-203/15 en C-698/15, ECLI:EU:C:2016:572 en ECLI:EU:C:2016:970, par. 99.
16. Ook het Belgische Grondwettelijk Hof heeft een prejudiciële vraag gesteld met betrekking tot de reikwijdte van *Tele2 Sverige AB* en *Watson*, met name of de door België nog steeds gehanteerde algemene verplichting voor de aanbieders van elektronische communicatiediensten om de verkeers- en locatiegegevens die door hen worden gegenereerd of verwerkt, te bewaren, in overeenstemming is met het Europees recht. Het Belgische Hof verwijst in die context met name naar het recht op veiligheid alsook op de staat rustende positieve verplichtingen om te voorzien in een wettelijk kader dat een effectief strafrechtelijk onderzoek en een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk maakt. Zie Grondwettelijk Hof België, Arrest nr. 96/2018 van 19 juli 2018. Zie voor een commentaar: Frank Verbruggen, Sofie Royer, Helena Severijns, 'Belgian Constitutional Court offers CJEU chance to explain its puzzling Tele2 Sverige AB-decision', *European Law Blog*, 1 oktober 2018, http://europeanlawblog.eu/2018/10/01/

alleen geldt voor een strafrechtelijke context (ter bestrijding van ernstige criminaliteit) of ook geldt in de context van nationale veiligheid. De verwijzende Britse klachtinstantie (*Investigatory Powers Tribunal*) uitte zijn bezorgdheid over de toepassing van deze strenge vereisten in een nationale veiligheidscontext en stelde daarom over de toepassing prejudiciële vragen aan het HvJ.

Nu is nationale veiligheid bij uitstek een bevoegdheid van de lidstaten. Art. 4(2) EU-Verdrag bepaalt zelfs uitdrukkelijk dat de nationale veiligheid de uitsluitende verantwoordelijkheid van elke lidstaat blijft. Verder is in dit verband van belang art. 5 EU-verdrag dat bepaalt dat de bevoegdheden van de EU zijn gebaseerd op het beginsel van bevoegdheidstoedeling (attributiebeginsel). Hieruit volgt dat de EU alleen die bevoegdheden kan uitoefenen die haar door de lidstaten middels de verdragen zijn toegekend. Het is de EU niet toegestaan zelf nieuwe bevoegdheden uit de bevoegdheden die zij al heeft af te leiden (implied powers). Het is dan maar de vraag of het HvJ zich kan uitspreken over de verenigbaarheid met het EU-recht van nationale (door lidstaten genomen) maatregelen ter bescherming van de nationale veiligheid.[17] Indien het HvJ zich hierover weigert uit te spreken, geldt op dit terrein uiteraard het vangnet van de jurisprudentie van het EHRM. Indien het HvJ zich wel uitspreekt, is het niet onwaarschijnlijk dat zij zich zal baseren op EHRM-rechtspraak, dat al meermaals beperkingen ingegeven door de nationale veiligheid heeft geadresseerd.[18] Indien het HvJ zich bevoegd acht zich uit te spreken over de aanhangige materie (toepasselijkheid E-privacyrichtlijn in nationale veiligheidscontext) is een belangrijke vervolgvraag wat dit betekent voor de reikwijdte en betekenis van art. 4 (2) van het EU-Verdrag (en mogelijk de reputatie en geloofwaardigheid van het HvJ). Voor dit artikel is van belang dat in beide gevallen de vraag rijst of het EVRM-recht en het EU-recht met elkaar gelijk lopen op dit punt.

3. Hoe verhoudt de jurisprudentie van het EHRM zich tot die van het HvJ? Relevante aanwijzingen uit *Big Brother Watch e.a.*

Hier staan wij stil bij de vraag hoe de jurisprudentie van het EHRM en het HvJ op het gebied van (massa) surveillance en privacy zich tot elkaar verhouden. De uitspraak van het EHRM in *Big Brother Watch e.a.* over bulkinterceptie en toegang tot opgeslagen gegevens bij communicatiediensten door inlichtingen- en veiligheidsdiensten staat hierbij centraal. Ook betrekken we relevante jurisprudentie van het HvJ. We gaan na of de jurisprudentie meer in de richting van convergentie of divergentie tussen het EHRM en het HvJ wijst. Daartoe zetten we de verschillende aanwijzingen op een rij aan de hand van drie kwesties die centraal staan in *Big Brother Watch e.a.*: (1) toegang tot opgeslagen gegevens bij communicatiediensten; (2) bulkinterceptie; (3) verwerving van metadata vs. inhoud.

reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/, waarin de auteurs het HvJ aanraden te rade te gaan bij de rechtspraak van het EHRM aangaande positieve verplichtingen. Zie voor een relevant arrest van het EHRM 2 december 2008, *K.U. t. Finland*, nr. 2872/02, ECLI:CE:ECHR:2008:1202JUD000287202, par. 49 ('Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.').

17. Het valt op te merken dat het HvJ zich in het verleden reeds heeft uitgesproken over nationale veiligheidssurveillance door *niet-lidstaten*, met name in de context van transfers van gegevens uit de EU naar derde staten, op basis van het toen geldende art. 25 van de Richtlijn Gegevensbescherming (1995). Die derde staten kunnen voor doeleinden van nationale veiligheid die data onderscheppen/verzamelen, en daarbij de rechten van EU-burgers schenden. Zie HvJEU 6 oktober 2015, *Maximilian Schrems t. Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650. Verzoek van de High Court (Ierland) om een prejudiciële beslissing. Prejudiciële verwijzing – Persoonsgegevens – Bescherming van natuurlijke personen in verband met de verwerking van die gegevens – Handvest van de grondrechten van de Europese Unie – Artikelen 7, 8 en 47 – Richtlijn 95/46/EG – Artikelen 25 en 28 – Doorgifte van persoonsgegevens naar derde landen – Beschikking 2000/520/EG – Doorgifte van persoonsgegevens naar de Verenigde Staten – Passend beschermingsniveau – Geldigheid – Klacht van een natuurlijke persoon van wie de gegevens vanuit de Europese Unie naar de Verenigde Staten zijn doorgegeven – Bevoegdheden van de nationale toezichthoudende autoriteiten. Zaak C-362/14. Bijgevolg kan het HvJ zich vreemd genoeg uitspreken over de verenigbaarheid van activiteiten van *buitenlandse* inlichtingen- en veiligheidsdiensten met het recht op gegevensbescherming, maar niet over de activiteiten van diensten van de lidstaten. Zie ook Francesca Bignami & Giorgio Resta, 'Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance' in E Benvenisti & G Nolte (eds.) *Community Interests Across International Law* (Oxford University Press 2017), p. 374-378, p. 371 ('Thus, the paradoxical situation obtains whereby EU institutions are called upon to review and potentially regulate spy agencies abroad, even though they do not exercise this same power over Member State spy agencies.').

18. Zie voor een – ietwat gedateerd – overzicht: I. Cameron, *National Security and the European Convention on Human Rights*, Martinus Nijhoff 2000; J.P. Loof, *Mensenrechten en staatsveiligheid: verenigbare grootheden? Opschorting en beperking van mensenrechtenbescherming tijdens noodtoestanden en andere situaties die de staatsveiligheid bedreigen* (Dissertatie, Faculteit der Rechtsgeleerdheid, Universiteit Leiden) nr. 96, in: Meijers-reeks. Nijmegen 2005 Wolf Legal Publishers.

3.1. Toegang tot opgeslagen gegevens bij communicatiediensten

Een aanwijzing voor een convergentielezing is het feit dat het EHRM de toegang tot gegevens bewaard door elektronische communicatiediensten uitsluitend aan de door het HvJ ontwikkelde criteria toetst (*Digital Rights Ireland Ltd en Seitlinger e.a., Tele2 Sverige AB en Watson*), en op basis daarvan direct een schending van art. 8 EVRM vaststelt. In *Big Brother Watch e.a.* stelt het EHRM als volgt: *'[D]omestic law, as interpreted by the domestic authorities in light of the recent judgments of the CJEU, requires that any regime permitting the authorities to access data retained by CSPs limits access to the purpose of combating "serious crime", and that access be subject to prior review by a court or independent administrative body … Accordingly, the Court finds that there has been a violation of Article 8 of the Convention.*'[19] Interessant genoeg baseerde het HvJ in *Tele2 Sverige AB en Watson* zichzelf op eerdere EHRM-rechtspraak[20], al gebruikte het EHRM de term 'ernstig misdrijf' (*serious crime*) niet expliciet in dat arrest. In ieder geval lijkt deze dialoog tussen het EHRM en het HvJ op een gelijk niveau van bescherming te wijzen. Nergens in *Big Brother Watch e.a.* stelt het EHRM dat zijn rechtspraak over massasurveillance qua beschermingsniveau afwijkt van die van het HvJ.

Inmiddels heeft het HvJ in de zaak *Ministerio Fiscal* (2018)[21], gewezen na *Big Brother Watch e.a.*, meer duidelijkheid gegeven over de interpretatie van de drempel van 'ernstig delict' in *Tele2 Sverige AB en Watson* voor toegang tot opgeslagen data bij communicatiediensten. Hierbij verwijst het HvJ overigens niet naar *Big Brother Watch e.a.* of enige andere EHRM-jurisprudentie. In de zaak *Ministerio Fiscal* beantwoordt het HvJ de prejudiciële vraag of alleen de strafmaat bepalend is voor een gerechtvaardigde inmenging in art. 7 en 8 Handvest van de Grondrechten of dat ook sprake moet zijn van een bijzondere aantasting van de betrokken rechten. Volgens het HvJ laat art. 15 lid 1 E-privacyrichtlijn (2002/58) toegang tot gegevens toe, niet alleen als het gaat om ernstige delicten, maar voor strafbare feiten in het algemeen. Hierbij geldt als voorwaarde dat het doel dat met de toegang wordt nagestreefd in verhouding staat tot de ernst van de inmenging in de betrokken grondrechten die deze ingreep meebrengt. Dit betekent dat in het concrete geval moet worden nagegaan of de gevraagde toegang tot bepaalde gegevens als ernstig moet worden aangemerkt.[22] Het HvJ wijst er hierbij op dat volgens het evenredigheidsbeginsel een ernstige inmenging alleen kan worden gerechtvaardigd als het doel ervan de bestrijding van ernstige criminaliteit is.[23] Bij een inmenging die niet als ernstig valt te kwalificeren, kan ook toegang voor de vervolging van strafbare feiten in het algemeen worden gevraagd.[24] In de kwestie *Ministerio Fiscal* was volgens het HvJ geen sprake van een ernstige inmenging nu het alleen ging om het verkrijgen van telefoonnummers en identiteitsgegevens van houders van simkaarten die gedurende een bepaalde periode met het IMEI-nummer van een gestolen mobiele telefoon waren geactiveerd. Daarentegen ging het niet om de communicatie die tot stand was gebracht of de locatie van de telefoon. Uit deze gegevens konden volgens het HvJ geen nauwkeurige conclusies over het privéleven van de betrokken personen worden getrokken. Daarom was toegang tot deze gegevens ook mogelijk buiten ernstige delicten.[25]

3.2. Bulkinterceptie

Op het punt van bulkinterceptie zijn de aanwijzingen voor convergentie of divergentie het minst eenduidig. In *Big Brother Watch e.a.* duiden enkele passages op een mogelijke divergentie met het EU-recht. Zo vindt het EHRM bulkinterceptie als zodanig een waardevol middel om de huidige dreigingen van terrorisme en ernstige criminaliteit het hoofd te kunnen bieden,[26] terwijl het HvJ in *Schrems* de door de VS uitgevoerde bulkinterceptie als een schending van het recht op privacy bestempelde.[27]

19. EHRM 13 september 2018, *Big Brother Watch e.a. t. het Verenigd Koninkrijk*, nrs. 58170/13, 62322/14, 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, par. 467-468.
20. EHRM 4 december 2015, *Zakharov t. Rusland*, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, *NJ* 2017/185, m.nt. Dommering, *EHRC* 2016/87, m.nt. Hagens, par. 260.
21. HvJEU 2 oktober 2018, *Ministerio Fiscal*, zaak C-207/16.
22. *Idem*, par. 58.
23. *Idem*, par. 56.
24. *Idem*, par. 57.
25. *Idem*, par. 59-61.
26. EHRM 13 september 2018, *Big Brother Watch e.a. t. het Verenigd Koninkrijk*, nrs. 58170/13, 62322/14, 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, par. 386.
27. HvJEU, *Schrems*, supra noot 17, par. 94. Het EHRM zelf vereiste voorheen dat het verzamelen van gegevens geïndividualiseerd moest zijn. Dit lijkt de legaliteit van massale gegevensverzameling (in bulk) te bemoeilijken. Zie EHRM 12 januari 2016, *Szabo and Vissy t. Hongarije*, nr. 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814, par. 73 ('A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation.'). Het EHRM verwees in dezelfde paragraaf van dat arrest naar de rechtspraak van het HvJ. Zie over de interpretatie van dit arrest ook Bignami en Resta, supra noot 17, p. 378 ('In this way the court seems to rule out, in the absence of a previous judicial authorization, the blanket collection of content and communications data referring to a wide range of persons and unrelated to a specific threat previously identified.'). Vergelijk met *Big Brother Watch e.a.*, par. 314 ('the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation'). Zie over de toelaatbaarheid van bulkinterceptie ook A. Peters, 'Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extraterritorial Surveillance' in Russell A. Miller (ed),

Theodore Christakis merkte in die context op dat er fragmentatie van het Europees recht (EU/EVRM) dreigt te ontstaan wat betreft de waarborgen met betrekking tot massasurveillance.[28] Die fragmentatie zou er kort gezegd uit bestaan dat het EHRM sneller dan het HvJ een oogje zal toeknijpen wanneer rechtsstatelijke waarborgen, zoals voorgaande rechtelijke toetsing, niet ten volle aanwezig zijn. Die flexibele houding lijkt goed tot uiting te komen in een door een andere kamer van het EHRM gewezen arrest van 19 juni 2018 in een andere surveillancezaak (*Centrum för Rättvisa t. Zweden*[29]). Het EHRM had in dat arrest wel wat aan te merken op de door de Zweedse overheid geboden waarborgen om misbruik te voorkomen, maar vond toch dat het Zweedse recht in het algemeen ('on the whole') voldeed[30], en dat bepaalde elementen van toezicht regelgevende tekortkomingen konden compenseren.[31] Deze 'holistische' benadering, waarbij het systeem als geheel wordt beoordeeld, en met name de uitkomst waartoe deze benadering leidde in *Centrum för Rättvisa*, viel niet bij iedereen in de smaak. Asaf Lubin bekritiseerde die 'lakse' houding van het EHRM als volgt:

> *'In the name of doing whatever it can to legitimize the Swedish foreign surveillance machine, it might have skewed the balance too far and inadvertently legitimized more dangerous mechanisms. Recognizing the need to tailor the right to privacy to account for the unique features of foreign surveillance should not result in de facto abandoning all of the court's important safeguards, nor should it lead us to cover our eyes to the practice's negative effects. Instead what is required is a careful and nuanced act of rebalancing. This requires high degrees of precision. In ruling on the Swedish case, the court unfortunately wielded its analysis less like a surgeon in an operating room and more like an elephant in a china shop.'*[32]

Wat de focus van dit artikel betreft, betekent *Centrum för Rättvisa* dat het EHRM wel eens een grotere appreciatiemarge (minder streng) dan het HvJ zou kunnen hanteren. Hierbij passen evenwel vier kanttekeningen. Ten eerste is de holistische aanpak van het EHRM zoals die naar voren komt in *Centrum för Rättvisa* niet nieuw. Hij werd al verondersteld in eerdere uitspraken: Ook al gebruikte het EHRM daarin niet de term 'on the whole', het Hof accepteerde wel de mogelijkheid dat bepaalde gebreken in het systeem met sterke waarborgen op andere plaatsen in dat systeem kunnen worden gecompenseerd.[33] Ten tweede gaat het in de genoemde jurisprudentie van het EHRM steeds om toetsing van surveillance wetgeving *in abstracto*, waarbij het EHRM expliciet de deur open laat om in geval van de toepassing van een daadwerkelijke onderzoeksmaatregel (interceptie) alsnog een schending te kunnen constateren. Ten derde lijkt de uitkomst in *Centrum för Rättvisa* eerder een uitzondering dan de regel. In eerdere zaken (bijvoorbeeld *Roman Zakharov t. Rusland* en *Szabo en Vissy t. Hongarije*) heeft

Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair (Washington and Lee University 2017), p. 162 ('big data [bulk interception] is not inherently disproportionate unless the data are collected without any discernible aim, such as the effort to interdict and combat terrorism and other serious crimes'). In *Szabo en Vissy t. Hongarije* stelde het EHRM uiteindelijk vast, met betrekking tot de door Hongarije genomen surveillancemaatregelen, dat '[g]iven that the scope of the measures could include virtually anyone, that the ordering is taking place entirely within the realm of the executive and without an assessment of strict necessity, that new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation, and given the absence of any effective remedial measures, let alone judicial ones, the Court concludes that there has been a violation of Article 8 of the Convention.' (par. 89).

28. T. Christakis, 'A Fragmentation of EU/ECHR Law on Mass Surveillance. Initial thoughts on the *Big Brother Watch* Judgment', *European Law Blog*, 20 september 2018, http://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/#more-4221.
29. EHRM 19 juni 2018, *Centrum för Rättvisa t. Zweden*, nr. 35252/08, ECLI:CE:ECHR:2018:0619JUD003525208.
30. *Idem*, par. 141.
31. *Idem*, par. 150.
32. https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/.
33. De mogelijkheid van uitwisselbaarheid van waarborgen en daarmee het balanceren van het systeem als geheel wordt ook onderschreven in de uitgebreide analyse van de EHRM-jurisprudentie over de eisen aan toezicht op inlichtingen- en veiligheidsdiensten van de Universiteit Leiden uit aug. 2015: via http://www.ctivd.nl/documenten/publicaties/2015/08/26/rapport-universiteit-leiden. Enkele recente voorbeelden: *Szabo en Vissy* (2016), *supra* noot 27 (par. 76-77: '... either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny....The ex-ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation.'); *Roman Zakharov* (2015), *supra* noot 20 (par. 249: '...judicial authorisation may serve to limit the law enforcement authorities' discretion in interpreting broad terms of ... 'events or activities endangering Russia's national, military, economic or ecological security' by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in every case.'; par. 271: '...the Court will therefore examine with particular attention whether the supervision arrangements provided by the Russian law are capable of ensuring that all interceptions are performed lawfully on the basis of proper judicial authorisation.').

deze aanpak van het EHRM steevast geleid tot vaststellingen van een schending van het EVRM. Dat lijkt ook weer aan de orde in *Big Brother Watch e.a.* Ten vierde laat het EHRM verdragsstaten een ruime beoordelingsvrijheid voor de keuze van het soort interceptieregime (bijvoorbeeld bulk of gericht), maar hanteert het een beperkte beoordelingsruimte voor wat betreft de invulling en uitvoering daarvan. Dat betekent dat alle heimelijke interceptie van communicatie, ongeacht of die gericht of in bulk plaatsvindt, een risico van misbruik inhoudt en daarom aan bepaalde minimumwaarborgen dient te voldoen.[34] Deze houden in dat zorg dient te worden gedragen voor toegankelijke en kenbare normen, en dat maatregelen slechts worden toegepast wanneer dit (strikt) noodzakelijk is in een democratische rechtsorde.[35] Ten aanzien van voorafgaande rechterlijke toestemming, een vereiste dat ook het HvJ in zijn jurisprudentie stelt voor toegang tot gegevens bij communicatiediensten, overweegt het EHRM in het kader van bulkinterceptie dat dit een belangrijke waarborg is en mogelijk zelfs een 'best practice', maar geen absoluut vereiste:

> *'(...) The Court has found it "desirable to entrust supervisory jurisdiction to a judge" because, as a result of the secret nature of the surveillance, the individual will usually be unable to seek a remedy of his or her own accord (see Roman Zakharov, cited above, § 233). However, that is not the case in every contracting State. (...) In this regard, the Venice Commission also noted that independent oversight may be able to compensate for an absence of judicial authorization. (...) Secondly, the Court has acknowledged that "the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system" (see Klass and Others, cited above, § 59), and one need only look at its most recent jurisprudence to find examples of cases where prior judicial authorisation provided limited or no protection against abuse. For example, in Roman Zakharov (...). Therefore, while the Court considers judicial authorisation to be an important safeguard, and perhaps even "best practice", by itself it can neither be necessary nor sufficient to ensure compliance with Article 8 of the Convention (see Klass and Others, cited above, § 56). Rather, regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse.'*[36]

Volgens rechters Pardalos en Eicke, die over de wijze van beoordelen een *dissenting* opinie bij de uitspraak *Big Brother Watch e.a.* schreven, had de toepassing van de toetsingsstandaard gebruikt in *Centrum för Rättvisa* het EHRM tot het besluit moeten brengen dat het VK art. 8 EVRM *niet* had geschonden (par. 25). Beide rechters stelden uitdrukkelijk dat het EU- en het EVRM-recht ter zake *niet* gelijk lopen: 'while there is some similarity in the language used by the two courts, the CJEU appears to have adopted a more prescriptive approach as regards the safeguards it considers necessary' (par. 22). Ze voegden daaraan toe dat het EHRM, anders dan het HvJ , ervoor kiest 'to review the impugned regime as a whole in order to evaluate the adequacy of the available safeguards' (par. 22). Volgens Pardalos en Eicke wijst de meerderheidsopinie in *Big Brother Watch e.a.* dus op (onwenselijke) convergentie tussen het EVRM en het EU-recht. Hun kritiek lijkt eruit te bestaan dat het EHRM in deze zaak opschuift naar de (strengere, minder flexibele) aanpak van het HvJ die uitgaat van een voorgeschreven set van waarborgen die aanwezig moet zijn, zonder open te staan voor weging van het systeem als geheel. Zoals wij hierboven al hebben aangegeven ('vier kanttekeningen'), behoeft de visie van de *dissenters* nuancering. In *Big Brother Watch e.a.* zijn er wel aanwijzingen dat het EHRM ook hier het systeem als geheel weegt en ruimte laat voor compenserende waarborgen waar dat kan. Het EHRM merkt immers op dat er geen onafhankelijke autorisatie bestaat, nu de lasten worden goedgekeurd door de minister van Binnenlandse Zaken, maar dat hierop, en op het functioneren van het 'surveillance' regime in het algemeen, voldoende toezicht bestaat door de *Interception of Communications Commissioner* en, in geval van een individuele klacht, door de *Investigatory Powers Tribunal* (IPT).[37] Een mogelijke verklaring voor het verschil in beoordeling tussen *Big Brother Watch e.a.* en *Centrum för Rättvisa* kan zijn dat het EHRM de geconstateerde gebreken in het Britse bulkinterceptiesysteem van een ernstiger niveau achtte, omdat ze de voorzienbaarheid/kwaliteit van de wetgeving betreffen, dan die in *Centrum för Rättvisa*.[38] In *Big Brother*

34. De minimumwaarborgen zijn: 'A description of the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of the measures; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed', daarnaast vindt het EHRM van belang dat voorzieningen bestaan voor voorafgaande onafhankelijke toetsing, notificatie en effectieve rechtsmiddelen, maar dit zijn geen minimumvereisten, o.a. *Centrum för Rättvisa*, par. 103/113, *Big Brother Watch e.a.*, par. 307/315.
35. O.a. *Centrum för Rättvisa*, par. 113, *Big Brother Watch e.a.*, par. 315.
36. *Big Brother Watch e.a.*, par. 318-320.
37. *Big Brother Watch e.a.*. par. 383.
38. In *Big Brother Watch e.a.* (par. 315-320) geeft het EHRM aan dat er volgens zijn vaste jurisprudentie een onderscheid bestaat tussen een aantal minimumwaarborgen voor interceptiesystemen (toegankelijkheid en voorzienbaarheid van wetgeving afbakening

Watch e.a. deden de gebreken zich voor in bepaalde noodzakelijke minimumwaarborgen, met name onvoldoende waarborgen m.b.t. de keuze van fibers (internetkabels) die werden afgetapt (fase 1) en de keuze van opgeslagen materiaal voor inhoudelijk onderzoek (fase 4), en een gebrek aan extern toezicht op de selectoren en zoektermen waarmee verworven materiaal wordt doorzocht (fase 3).[39] In *Centrum för Rättvisa* bestonden de gebreken vooral uit een onvoldoende duidelijke regeling voor de uitwisseling van (persoons)gegevens uit 'signals intelligence' met buitenlandse inlichtingen- en veiligheidsdiensten, een gebrekkige notificatievoorziening, de afwezigheid van een rechterlijke klachtvoorziening en het niet motiveren van een klachtoordeel waardoor klager geen uitsluitsel krijgt of zijn communicatie daadwerkelijk is onderschept. In dat geval was er in *Big Brother Watch e.a.* geen ruimte voor compenserende waarborgen.[40] Het EHRM toetst aan een uitgebreide set van vereisten en neemt daarbij de daadwerkelijke werking van het interceptiesysteem, inclusief alle *checks and balances* en concrete aanwijzingen (of gebrek daaraan) voor feitelijk misbruik, als grondslag voor zijn beoordeling. Afgaande op de gewogen benadering en gehanteerde vereisten van het EHRM op het terrein van massasurveillance in vergelijking met het HvJ lijkt er weinig grond voor de stelling dat het HvJ strenger is dan het EHRM.

3.3. Verwerving van metadata vs inhoud

In *Big Brother Watch e.a.* stelt het EHRM dat de verwerving van metadata (*related communications data*) *even*, en zo niet *meer*, ingrijpend kan zijn als de verwerving van inhoud (*content*). Metadata betreft onder meer informatie over de locatie van een mobiele telefoon en van zender en ontvanger, *routing*- en *webbrowsing*-informatie, of informatie met betrekking tot het *online* traceren van een postpakket. Het EHRM stelt ter zake:

> *'[T]he content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with.'*[41]

Het verwerven van metadata dient volgens het EHRM dan ook omkleed te zijn met voldoende waarborgen, wat *in casu* niet het geval was: de Britse wetgeving had metadata volledig vrijgesteld van de waarborgen die van toepassing zijn op het doorzoeken onderzoeken van inhoud (para. 357). Deze benadering lijkt in contrast te staan met de op het eerste gezicht minder strenge benadering van het HvJ wat dataretentie betreft. In *Digital Rights Ireland Ltd en Seitlinger e.a.* stelde het HvJ immers als volgt, met betrekking tot de bewaring van metadata op basis van een (indertijd toepasselijke) EU-Richtlijn over gegevensbewaring door elektronische communicatiediensten:[42]

> *'Wat de wezenlijke inhoud van het fundamentele recht op eerbiediging van het privéleven en de andere door artikel 7 van het [EU-Handvest van de Grondrechten] erkende rechten betreft, moet worden vastgesteld dat de door richtlijn 2006/24 voorgeschreven bewaring van gegevens weliswaar een bijzonder zware inmenging in deze rechten vormt, maar niet raakt aan de inhoud ervan, aangezien deze richtlijn, zoals blijkt uit artikel 1, lid 2, ervan, niet de mogelijkheid biedt om kennis te nemen van de inhoud zelf van de elektronische communicaties.'*[43]

Na de zaak *Digital Rights Ireland Ltd en Seitlinger e.a.*, stelt het HvJ in *Tele2 Sverige AB en Watson*, metadata, voor wat betreft de ernst van een inmenging in het privéleven, gelijk aan inhoud van communicatie. Volgens het HvJ kunnen uit de opgeslagen

van bevoegdheden en toepassingsbereik, concretisering duur, verlenging en beëindiging van maatregelen, zorgvuldige procedures voor opslag, toegang, onderzoek, gebruik, delen/verstrekken, bewaren, vernietigen van gegevens), en een aantal andere relevante elementen die geen minimumvereisten zijn (onafhankelijke autorisatie, notificatie, effectieve rechtsmiddelen).

39. *Idem*, par. 346-347.
40. Overigens valt op de beoordeling van het EHRM van de tekortkomingen in de Zweedse regeling inzake samenwerking en gegevensuitwisseling met buitenlandse diensten dat deze worden gecompenseerd door het toezicht op de Zweedse sigint-dienst, wel het nodige af te dingen, omdat niet duidelijk is in hoeverre dat toezicht (achteraf) betrekking heeft op de samenwerking met buitenlandse diensten. Het toezicht is bovendien beperkt tot de Zweedse sigint-dienst en kan zich niet uitstrekken tot de ontvangende partij, bijvoorbeeld of deze op een rechtmatige en zorgvuldige wijze met de gegevens omgaat. Ook blijkt niet dat er voor de uitwisseling van gegevens onafhankelijke toestemming vereist is (*Centrum för Rättvisa*, par. 153-161), zie ook combi-annotatie M. Hagens in *EHRC* 2018/208 bij *Big Brother Watch e.a* en 2018/196 bij *Centrum för Rättvisa*.
41. *Big Brother Watch e.a.*, par. 356.
42. 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, *OJ L 105, 13.4.2006, p. 54–63.*
43. HvJ EU 8 april 2014, *Digital Rights Ireland Ltd* en *Seitlinger e.a.*, C-293/12 en C-594/12, ECLI:EU:C:2014:238, par. 39.

metadata, zoals verkeers- en locatiegegevens[44], zeer precieze conclusies 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. Hierbij verwijst het HvJ overigens naar analogie naar het arrest *Digital Rights Ireland Ltd en Seitlinger e.a.* (punten 26-27). Het HvJ benadrukt dat aan de hand van de bewaarde metagegevens het profiel van de betrokken personen kan worden bepaald. Deze informatie is wat betreft het recht op bescherming van het privéleven, even gevoelig als de inhoud van telecommunicatie.[45] Dat gaat echter niet zover dat het HvJ vindt 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 EU-Handvest van de Grondrechten). Wel kan een algemene en ongedifferentieerde bewaarplicht het gevoel van permanente surveillance geven en bestaat het risico van een *chilling effect* op het gebruik van elektronische communicatiemiddelen, zoals de wijze waarop iemand zich uit of juist daarvan afziet.[46] Op grond van het evenredigheidsbeginsel brengt dit het HvJ ertoe beperkingen te stellen aan de omvang van de bewaarplicht voor private communicatiediensten (dat wil zeggen gericht en in relatie tot het doel van bestrijding van ernstige criminaliteit[47]) en bepaalde waarborgen te vereisen op het terrein van toegang tot deze gegevens en gegevensbeveiliging.

Zowel het EHRM als het HvJ onderkennen thans het potentieel inbreukmakende karakter van (bulk)metadata van communicatie. Er zijn aanwijzingen dat zij elkaars jurisprudentie daarbij goed in het oog houden. Verder gaan zij steeds vaker uit van de mate van inbreuk op de persoonlijke levenssfeer van bepaalde gegevens en niet van het onderscheid metadata vs. inhoud. In *Ministerio Fiscal* overweegt het HvJ dat niet alle soorten metadata een ernstige inbreuk op de persoonlijke levenssfeer inhouden.[48] In *Big Brother Watch e.a.* gaat het EHRM mogelijk nog iets verder dan het HvJ in *Tele2 Sverige AB en Watson* door te overwegen dat metadata mogelijk meer inbreukmakend kan zijn dan inhoud van communicatie. Verder is van belang te wijzen op de omstandigheid dat het EHRM in de zaak *Big Brother Watch e.a.* in zijn beoordeling van de toegang van de Britse geheime diensten tot opgeslagen communicatiegegevens bij private communicatiediensten de criteria van het HvJ hanteert (besproken in paragraaf 3.1). Wat betreft de ingrijpende aard van toegang tot metagegevens, en de vereiste waarborgen ter zake, lijkt dan ook sprake van convergentie tussen HvJ en EHRM.

4. Afsluitende opmerkingen

Op dit moment is bij het HvJ een verzoek om een prejudiciële beslissing aanhangig in een Britse zaak (*Privacy International*) over de vraag of onderdelen van de nieuwe Britse surveillancewetgeving (*Investigatory Powers Act 2017*), ter bescherming van de nationale veiligheid, voldoen aan de vereisten die het HvJ in de zaken *Tele2 Sverige AB en Watson* stelde. In *Big Brother Watch e.a.* heeft het EHRM net, als sluitstuk van zijn jarenlange jurisprudentie over surveillance en privacy, een oordeel gegeven over de vorige Britse surveillancewetgeving. Dit alleen al maakt de vraag relevant hoe de normen van beide gerechtshoven zich tot elkaar verhouden.

Voorgaande exercitie illustreert dat het niet zo gemakkelijk is een eenduidig antwoord te geven op de vraag of de EU- en EVRM-waarborgen inzake massasurveillance met elkaar corresponderen. Desondanks lijkt de huidige stand van de jurisprudentie te wijzen op een grote mate van wederzijdse beïnvloeding dan wel convergentie. Hoewel de structuren van de Europese Unie en van het EVRM onafhankelijk van elkaar functioneren vanuit een eigen mandaat en focus, wijzen recente uitspraken van beide gerechtshoven op een nauwe verwevenheid en in essentie gelijke standaarden. Toch valt over het beschermingsniveau dat beide structuren bieden (nog) geen definitief uitsluitsel te geven. Mogelijk kan de Grote Kamer van het EHRM (als *Big Brother Watch e.a.* wordt doorverwezen, dat was op het moment van schrijven nog niet duidelijk) of het HvJ in de prejudiciële beslissing in *Privacy International* hierover duidelijkheid scheppen. Met name zou het HvJ in die zaak of andere zaken kunnen vaststellen – al is dat geenszins zeker – dat het niveau van bescherming die het EU-recht in surveillance biedt hoger is dan die geboden door het EVRM. Het EU-Handvest van de Grondrechten bevat immers naast een recht op privacy (art. 7 Handvest) een specifiek recht op gegevensbescherming (art. 8 Handvest), terwijl het EVRM 'slechts' een recht op privacy voorziet (art. 8 EVRM, waaronder overigens wel gegevensbescherming wordt gevat), en voorziet in een minimumniveau van bescherming.

44. Gegevens over communicatie, denk aan: de bron en de bestemming van een communicatie, de datum, het tijdstip, de duur en de aard van de communicatie, de communicatieapparatuur van de gebruikers en de locatie van de mobiele communicatieapparatuur. Die gegevens omvatten onder meer de naam en het adres van de abonnee of van de geregistreerde gebruiker, het telefoonnummer van de oproeper en het opgeroepen nummer en een IP-adres voor de internetdiensten. HvJ EU 21 december 2016, *Tele2 Sverige AB* en *Watson*, C-203/15 en C-698/15, ECLI:EU:C:2016:572 en ECLI:EU:C:2016:970, par. 98.
45. HvJ EU 21 december 2016, *Tele2 Sverige AB* en *Watson*, C-203/15 en C-698/15, ECLI:EU:C:2016:572 en ECLI:EU:C:2016:970, par. 99.
46. *Idem*, par. 100-101.
47. Zie op dit punt de verfijning in de zaak *Ministerio Fiscal*, besproken in paragraaf 3.1 van dit artikel.
48. HvJ EU 2 oktober 2018, *Ministerio Fiscal*, zaak C-207/16, par. 56-57.