

EHRM 13 september 2018, nrs. 58170/13, 62322/14 en 24960/15, [ECLI:CE:ECHR:2018:0913JUD005817013](https://eclii.europa.eu/eur/cour/cour_echr/2018/0913jud005817013), *Computerrecht* 2018/252, m.nt. J.J. Oerlemans (*Big Brother Watch t. Verenigd Koninkrijk*)¹

Noot

1. De *Big Brother Watch*-uitspraak is een – wat de Amerikanen noemen – ‘*landmark case*’ van het Europees Hof voor de Rechten van de Mens (hierna: EHRM). In *Big Brother Watch* komt het EHRM tot de conclusie dat het Verenigd Koninkrijk inbreuk heeft gemaakt op artikel 8 (recht op privacy) en artikel 10 (vrijheid van meningsuiting) van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM), vanwege de inzet van ‘bulkinterceptie’ door de Britse communicatie-inlichtingendienst. Deze annotatie gaat kort na hoe het EHRM tot deze beslissing kwam en welke consequenties de uitspraak eventueel heeft voor de regeling van bulkinterceptie in Nederland, in de vorm van de bijzondere bevoegdheid van ‘onderzoeksopdrachtgerichte interceptie’ (artt. 48-50 Wiv 2017).
2. Allereerst is van belang dat het Straatsburgse Hof met deze uitspraak opnieuw laat zien dat de toepassing van bulkinterceptie noodzakelijk kan zijn in een democratische samenleving.² Het was niet een gegeven dat het EHRM bulkinterceptie als bijzondere bevoegdheid toelaatbaar zou vinden. Dat heeft te maken met de uitspraken in 2014 en 2016 van het Hof van Justitie van de Europese Unie (HvJ EU) met betrekking tot dataretentie, waarin het HvJEU aangeeft dat een generieke bewaarplicht van telecommunicatiegegevens in strijd is met het recht op privacy en de bescherming van persoonsgegevens.³ Als het EHRM zou aansluiten bij de strengere lijn van het HvJ EU met betrekking tot de grootschalige opslag van gegevens (ook van personen die niet direct onder de aandacht van de diensten staan), dan had het ook tot de conclusie kunnen komen dat de vergaande bevoegdheid disproportioneel en daarmee niet-noodzakelijk in een democratische samenleving zou zijn. In plaats daarvan legt het EHRM uit dat– mede gezien de hoge dreiging van terroristische aanslagen en technologische ontwikkelingen die het werk van inlichtingen- en veiligheidsdiensten beïnvloeden - aan lidstaten een ruime beoordelingsruimte toekomt om te bepalen op welke wijze de nationale veiligheid beschermd kan worden, waarbij staten ervoor kunnen kiezen bulkinterceptie toe te passen om de ongekende bedreigingen van nationale veiligheid te kunnen identificeren (par. 314). Het Hof stelt vast dat, anders bij gerichte interceptie, bulkinterceptie aan de voorkant meer ongericht is. Voor de uitoefening van de ingrijpende bevoegdheid moeten echter strikte regels gelden, in het bijzonder bij het nader analyseren van de onderschepte communicatie (par. 329).
3. Het EHRM vereist in zijn toets aan art. 8 EVRM dat de nationale wetgeving van verdragstaten aan bepaalde kwalitatieve vereisten voldoet (dat het ‘*in accordance with the law*’ is). Het hof sluit daarbij aan bij de zes criteria toe die zijn geformuleerd in de

¹ Jan-Jaap Oerlemans is verbonden als onderzoeker aan eLaw, het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden. Hij is werkzaam als onderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Deze annotatie is op persoonlijke titel geschreven.

² Het EHRM achtte al eerder bulkinterceptie toelaatbaar in *Weber Saravia t. Duitsland* (EHRM 26 juni 2006, nr. 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400, *EHRC* 2007/13 m.nt. J.P. Loof) en recentelijk in *Centrum för Rättvisa t. Zweden* (EHRM 19 juni 2018, nr. 35252/08, ECLI:CE:ECHR:2018:0913JUD005817013, *EHRC* 2018/208, m.nt. M. Hagens).

³ HvJ EU 8 april 2014, C293/12, C-594/12, ECLI:EU:C:2014:238, *EHRC* 2014/140 m.nt. M.E. Koning (*Digital Rights t. Ierland*) en HvJ EU 21 december 2016, C-203/15 en C698/15, ECLI:EU:C:2016:970, *EHRC* 2017/79, m.nt. M.E. Koning (*Tele2 Sverige AB t. Post-och telestyrelsen* en *Secretary of State for the Home Department t. Tom Watson e.a.*).

Zhakarov-zaak⁴, maar past deze criteria wel aan zodat deze passen bij de bijzondere bevoegdheid van bulkinterceptie (par. 320). Dat betekent bijvoorbeeld dat niet wordt geëist dat alleen gegevens worden verzameld als er al een 'redelijke verdenking' bestaat. Het EHRM toetst in de uitspraak met betrekking tot artikel 8 EVRM of de Britse wetgeving voldoet aan de volgende set aan waarborgen: (1) toegankelijkheid van de wetgeving, (2) afbakening toepassingsbereik van '*signals intelligence*', (3) de duur, verlenging en beëindiging van de bulkinterceptie, (4) onafhankelijke autorisatie bij onderschepping van de communicatie en voldoende toezicht om effectieve en voortdurende controle op het interceptieproces uit te oefenen, (5) zorgvuldige procedures voor opslag, toegang, onderzoek, gebruik en vernietiging van onderschepte persoonsgegevens, (6) voorwaarden voor het verstrekken van gegevens aan andere inlichtingen- en veiligheidsdiensten en (7) notificatie en voldoende rechtsmiddelen bij het vermoeden van schendingen bij de toepassing van bulkinterceptie.

4. Het EHRM acht de Britse wetgeving op de meeste elementen in orde, zoals de duur van de interceptie (par. 360), de procedures voor opslag, toegang, onderzoek en gebruik (par. 364), de procedures voor het delen met andere partijen (par. 369) en het verwijderen en vernietigen van data (par. 374). Onder de (oude) Britse wetgeving was de toepassing van de bevoegdheid tot bulkinterceptie niet aan een onafhankelijke autorisatie onderhevig. De lasten werden namelijk goedgekeurd door de minister van Binnenlandse Zaken. Desondanks meent het Hof dat op het functioneren van het '*surveillance*'-regime in het algemeen voldoende toezicht bestaat door de '*Interception of Communications Commissioner*' en (bij klachten) het '*Investigatory Powers Tribunal*' (par. 383). Voorafgaande autorisatie door een rechter is een 'best practice', maar door een onafhankelijke instantie mag ook (behalve bij advocaten en journalisten). Voldoende rechterlijk toezicht achteraf kan ook mogelijk compensatie bieden voor mogelijke gebreken in de toestemmingsverlening.⁵
5. Uiteindelijk komt het EHRM in *Big Brother Watch* toch tot een schending van art. 8 EVRM vanwege (1) het ontbreken van effectief toezicht op het geautomatiseerd doorzoeken van de verworven gegevens aan de hand van selectoren en zoektermen en (2) het ontbreken van effectieve waarborgen met betrekking tot de analyse van de metadata van geïntercepteerde communicatie (par. 338). In het bulkinterceptieregime in het Verenigd Koninkrijk worden de volgende vier fasen onderscheiden: (1) interceptie van een aantal glasvezel '*fibers*' waarover naar verwachting internationale communicatie wordt vervoerd, (2) het '*realtime*' filteren en vernietigen van niet-relevante onderschepte communicatie, (3) het geautomatiseerd doorzoeken van de verworven gegevens aan de hand van selectoren en zoektermen en (4) het onderzoek van het bewaarde materiaal door een analist (par. 329). Volgens het EHRM zijn er onvoldoende waarborgen in fase 3 en 4.
6. Bij het proces van het geautomatiseerd doorzoeken van de verworven gegevens aan de hand van selectoren en zoektermen (fase 3) wordt ook de inhoud van communicatie aan de hand van zogenoemde '*selectors*' en zoektermen opgeslagen. Het Hof overweegt dat de selectoren en zoektermen die worden gebruikt om verworven materiaal te onderzoeken onderhevig moeten zijn aan extern toezicht, maar deze selectoren en zoektermen behoeven zelf niet te worden opgenomen in het verzoek tot inzet van de bevoegdheid (par. 340). In het Britse systeem ontbreekt voldoende onafhankelijk

⁴ EHRM 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, *Computerrecht* 2016/86, m.nt. S.J. Eskens, par. 231 (*Roman Zakharov t. Rusland*).

⁵ EHRM 19 juni 2018, nr. 35252/08, ECLI:CE:ECHR:2018:0913JUD005817013, par. 133 (*Centrum för Rättvisa t. Zweden*). Zie ook de annotatie van Hagens bij de zaken van *Centrum för Rättvisa t. Zweden* en *Big Brother Watch t. Verenigd Koninkrijk* in EHRC 2018/208.

toezicht op fase 3 van het bulkinterceptieproces (par. 340 en 346-347). De interne en externe audits die plaatsvinden op de naleving van de waarborgen in wetgeving omtrent de verwerking van gegevens, compenseert niet het gebrek aan toezicht (par. 344-345).

7. Bij de analyse van de opgeslagen geïntercepteerde communicatie door een analist (fase 4), bestaan volgens het Hof in het Britse systeem te weinig waarborgen. Het Hof is bezorgd dat deze metadata zonder restrictie kunnen worden onderzocht (par. 355). Het EHRM zet uiteen dat met de analyse van metadata een zware inmenging met het recht op privacy van de betrokkenen kan plaatsvinden, omdat metadata informatie bevatten over de identiteit van beide communicerende partijen, hun geolocatie en gebruikte apparatuur. Bij de opslag en analyse van deze gegevens in bulk (een zeer grote hoeveelheid gegevens) wordt de inmenging met het recht op privacy groter, omdat het daarmee mogelijk is de contacten van een persoon, bewegingen en locaties, internetgeschiedenis en communicatiepatronen in kaart te brengen (par. 353-355). Het Verenigd Koninkrijk heeft volgens het EHRM geen juiste balans gevonden door deze categorie van gegevens uit te sluiten van de waarborgen in de wetgeving (par. 357).
8. Bij toepassing van de overwegingen van het Hof op de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017), lijkt de regeling voor 'onderzoekopdrachtgerichte interceptie' in artt. 48-50 Wiv 2017 op hoofdlijnen in orde. Het stelsel voor bulkinterceptie uit beide landen is op hoofdlijnen vergelijkbaar.⁶ Wel overweegt het Hof in *Big Brother Watch* dat de bulkinterceptie in het Verenigd Koninkrijk '*foreign focused*' is. Voor het binnenland bestaan meer mogelijkheden om gericht de benodigde gegevens te verzamelen voor de taakuitvoering. Op grond van de Britse wetgeving mogen zelfs geen gegevens via bulkinterceptie in het binnenland worden vergaard die met gerichte interceptie kunnen worden verkregen (par. 343). In Nederland hebben de ministers van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Defensie hebben in een Kamerbrief n.a.v. van het raadgevend referendum toegezegd dat het vrijwel is uitgesloten dat onderzoekopdrachtgerichte interceptie op de kabel de komende jaren wordt ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland.⁷ Dat geldt met uitzondering van onderzoek in het kader van '*cyber defence*', omdat bij digitale aanvallen misbruik wordt gemaakt van de Nederlandse digitale infrastructuur en OOG-interceptie op de kabel in het binnenland noodzakelijk kan zijn om dit te onderkennen. In de Wiv 2017 of de Beleidsregels Wiv 2017 is geen vereiste opgenomen dat de inzet van de bijzondere bevoegdheid – met uitzondering van de inzet in het kader van cyber defence – zich uitsluitend richt op binnenlands verkeer. Het is denkbaar dat dit onderdeel is van de uit te voeren proportionaliteits- en subsidiariteitstoets bij de inzet van bijzondere bevoegdheden (art. 26 Wiv 2017).
9. De bewaartermijn van drie jaar voor gegevens uit onderzoekopdrachtgerichte interceptie is in Nederland langer dan de bewaartermijn van twee jaar in de Britse wetgeving (par. 371-372). De bewaartermijn is volgens het Hof één van de elementen die wordt meegenomen bij de toetsing van de kwaliteit van wetgeving. In Nederland moeten gegevens waarvan is vastgesteld dat ze niet-relevant zijn voor het onderzoek, dan wel enig ander lopend onderzoek vallend onder de taken van de AIVD of de MIVD, terstond

⁶ Zie over het 'drie-fasen stelsel' voor OOG-interceptie in Nederland: *Kamerstukken II 2016/17*, 34588, 3, p. 90-124. Zie ook J.J. Oerlemans & M. Hagens, 'De Wet op de inlichtingen- en veiligheidsdiensten 2017: een technologisch gedreven wet', *Computerrecht* 2018/111, nr. 3, p. 130-141 en P.J.F. Koop, 'De Snowden-onthullingen en ongerichte interceptie onder de Wiv 2017', *Justitiële verkenningen* 2018, nr. 1, p. 133-147. Bij vergelijking met het stelsel in het Verenigd Koninkrijk, valt op dat in Nederland bij selectie (art. 50 lid 1 sub a Wiv 2017) een 'hard' onderscheid plaats vindt op de geïntercepteerde communicatie. Bij selectie wordt de inhoud van de geïntercepteerde communicatie opgeslagen en gelden aparte waarborgen (functie- taakscheiding) om kennis te nemen van de inhoud van de communicatie.

⁷ Kamerbrief van 25 april 2018 n.a.v. het raadgevend referendum Wiv 2017.

worden vernietigd. De niet-onderzochte gegevens moeten uiterlijk na drie jaar worden vernietigd (art. 48 lid 5 Wiv 2017). Naar aanleiding van het raadgevend referendum is in artikel 4 van de Beleidsregels Wiv 2017 vastgesteld dat aan de minister van BZK of Defensie na één jaar toestemming moet worden gevraagd de verworven gegevens uit interceptie op de kabel, voor zover zij nog niet op relevantie zijn beoordeeld, nog een jaar te bewaren (met de mogelijkheid van twee keer verlenging).

10. In Nederland is bij selectie (het opslaan van de inhoud van geïntercepteerde communicatie ter nadere kennisname van deze gegevens), in tegenstelling tot in het (oude) Britse stelsel, wél een voorafgaande onafhankelijke toetsing door de Toetsingscommissie Inzet Bevoegdheden (TIB) vereist.⁸ Ter uitvoering van de bijzondere bevoegdheid tot selectie worden selectiecriteria vastgesteld. Deze selectiecriteria zien bijvoorbeeld op technische kenmerken van personen, organisaties en aan een nader omschreven onderwerp gerelateerde trefwoorden.⁹ De vast te stellen selectiecriteria dienen te worden voorzien van een toereikende motivering, dat wil zeggen toereikend voor het doel van de selectie in relatie tot het onderzoek waarvoor de selectie plaatsvindt. Zoals in punt 4 duidelijk is gemaakt, acht het Hof een effectieve toetsing (zowel op papier als in de praktijk) door een onafhankelijke instantie ook mogelijk (in plaats van een rechterlijke toets). Daarbij is het voor de beoordeling van de onafhankelijkheid van een dergelijke instantie relevant dat ten minste twee van de drie leden van TIB, waaronder de voorzitter, ten minste zes jaar ervaring moeten hebben met de functie van rechterlijk ambtenaar in de rechtspraak.¹⁰
11. In Nederland is bij de uitvoering van ‘geautomatiseerde data-analyse’ (metadata-analyse) op geïntercepteerde communicatie uit bulkinterceptie de inzet van een bijzondere bevoegdheid vereist, voor zover de geautomatiseerde data-analyse is gericht op het identificeren van personen en organisaties.¹¹ In dat geval moet toestemming worden verkregen van de betrokken minister en vindt een rechtmatigheidstoets van de TIB plaats. Het gebrek aan restricties bij metadata-analyse uit gegevens verkregen uit bulkinterceptie was één van de twee redenen waarom in *Big Brother Watch* sprake was van een schending van art. 8 EVRM (zie punt 7). Voor andere vormen van ‘geautomatiseerde data-analyse’ (metadata-analyse) die niet zijn gericht op de identificatie van personen en organisaties, zoals het in kaart brengen van bewegingen op basis van locatiegegevens en websitebezoeken van een specifieke target, is in Nederland *niet* de inzet van een bijzondere bevoegdheid vereist (met toestemming van de minister en een toets van de TIB). Art. 60 lid 2 Wiv 2017 schrijft alleen voor dat het bij geautomatiseerde data-analyse niet is toegestaan uitsluitend op basis van de resultaten van een gegevensverwerking ‘maatregelen’ te bevorderen of te treffen.
12. Ten slotte zijn ook de overwegingen van het Hof met betrekking tot art. 10 EVRM (het recht op de vrijheid van meningsuiting) interessant. In *Big Brother Watch* stelden de klagers dat bulkinterceptie ook inbreuk kan maken op de door art. 10 EVMR beschermde bronbescherming voor journalisten. Het EHRM overweegt dat bij bulkinterceptie op voorhand niet duidelijk is dat journalistieke communicatie wordt onderzocht. In de eerste fase uit het Britse interceptiestelsel is dan ook geen sprake van een schending van art. 10 EVRM (par. 492). Wel moeten specifieke waarborgen gelden als eenmaal sprake is van de nadere analyse van gegevens met betrekking tot de communicatie van journalisten. Gelet op het potentiële ‘chilling effect’ van de mogelijkheid van dit soort

⁸ Art. 50 lid 1 sub a Wiv 2017.

⁹ *Kamerstukken II 2016/17*, 34588, 3, p. 108.

¹⁰ Zie art. 33 lid 2 Wiv 2017. Zie ook EHRM 19 juni 2018, nr. 35252/08, ECLI:CE:ECHR:2018:0913JUD005817013, par. 156-159 (*Centrum för Rättvisa t. Zweden*).

¹¹ Art. 50 lid 1 sub b jo lid 4 Wiv 2017.

analyses van gegevens, constateert het Hof op dit punt een schending van art. 10 EVRM (par. 495). In de Britse wetgeving geldt slechts extra bescherming als gegevens worden geanalyseerd met het doel om *journalistieke bronnen* te identificeren (par. 499). Het EHRM vereist bij het vergaren van communicatiegegevens met betrekking tot journalisten een rechterlijke of onafhankelijke controle en niet alleen met betrekking tot het achterhalen van journalistieke bronnen. Om deze reden constateert het Hof dat sprake is van een schending van art. 10 EVRM (par. 499).

13. In de Wiv 2017 is extra bescherming voor journalisten geregeld in art. 30 lid 2 Wiv 2017. Daar staat in dat toestemming van de Rechtbank Den Haag is vereist op verzoek van de betrokken minister, waarbij de uitoefening van bijzondere bevoegdheden (inclusief OOG-interceptie) '*kan* leiden tot verwerving van gegevens inzake de bron van de journalist'. De bepaling is wat dubbelzinnig geformuleerd, omdat de indruk kan ontstaan dat toestemming van een rechtbank slechts is vereist voor zover de bevoegdheid het doel heeft de bron van een journalist te achterhalen. In art. 30 lid 2 Wiv 2017 staat echter "*kan* leiden tot". Het EHRM maakt in par. 499 in ieder geval duidelijk dat de waarborg van een rechterlijke toets geldt bij onderzoek van gegevens over de communicatie van journalisten, ook als dit onderzoek als zodanig niet is gericht op het achterhalen van de bron van de journalist. Dit kan wellicht duidelijker worden gemaakt in het wetsvoorstel 'Wijziging Wiv 2017', dat recentelijk [in consultatie is geweest](#).