Bulkbevoegdheden en strafrechtelijk onderzoek

Galič, Maša

published in
Tijdschrift voor Bijzonder Strafrecht en Handhaving
2022

DOI (link to publisher)
10.5553/TBSenH/229567002022008002007

document version
Publisher's PDF, also known as Version of record

Trending Topics

Bulkbevoegdheden en strafrechtelijk onderzoek

Lessen uit de jurisprudentie van het EHRM voor de normering van grootschalige data-analyse

Dr. M. Galič*

1. Inleiding

Het nieuws wemelt de laatste jaren van berichten over grootschalige hack-operaties in strafrechtelijke onderzoeken. Denk bijvoorbeeld aan de operaties tegen *EncroChat*, *Sky ECC* en *Anom*.[1] Deze operaties zijn niet gericht op de computers van een specifiek individu of een specifieke groep mensen, zoals gebruikelijk is bij strafvorderlijke bevoegdheden. Bij de zojuist benoemde hack-operaties is zelfs het tegendeel uitgangspunt: op grote schaal worden gegevens verkregen door willekeurig in te breken op de cryptotelefoons van *alle gebruikers* van de encryptiedienst. In het geval van EncroChat resulteerde dit in het hacken van meer dan 32.000 gebruikers van deze cryptotelefoons en de verkrijging van een enorme schat aan gegevens – waaronder 25 miljoen berichten, afbeeldingen, notities, locatiegegevens en IMEI-nummers – die vervolgens voor verder strafrechtelijk onderzoek kunnen worden gebruikt.[2] Daarom spreken we in deze zojuist genoemde gevallen van 'bulk-hacking' in plaats van gewone of 'gerichte hacking'.

Bulkbevoegdheden, zoals bulk-hacking of bulkinterceptie van communicatie, zijn gewoonlijk voorbehouden aan inlichtingendiensten in het kader van de nationale veiligheid en zijn doorgaans gericht op buitenlandse communicatie.[3] In de afgelopen decennia is er echter een vervaging gaande tussen de functies van de politie en de inlichtingendiensten.[4] De politie probeert zich om te vormen tot een informatiegestuurde organisatie, waarbij 'datagedreven opsporing' (of *intelligence led policing*) en preventieve bulkonderzoekstechnieken een steeds belangrijkere rol spelen.[5] De bulk-hackbevoegdheid in artikel 126uba van het Wetboek van Strafvordering (Sv) is een recent voorbeeld van deze bredere transformatie van het politiewerk.

De voordelen van een dergelijke transformatie zijn bekend: zij kan met name leiden tot effectievere onderzoeken en het voorkomen van strafbare feiten.[6] De ongekende mogelijkheden van de politie om enorme hoeveelheden communicatie en andere soorten gegevens met betrekking tot (min of meer) willekeurige groepen

* Dr. M. Galič is universitair docent Privacy en Straf(proces)recht aan de Vrije Universiteit Amsterdam.

1 Zie bijv. J. Cox, 'How Police Secretly Took Over a Global Phone Network for Organized Crime', *Vice* 2 juli 2020; J. Peters, 'Politie noemt het hacken van Sky ECC "één grote tap op de onderwereld"', nu.nl 9 maart 2021; L. Hay Newman, 'The FBI's Anom Stunt Rattles the Encryption Debate', *Wired* 6 november 2021.

2 Landgericht Berlin 1 juli 2021, ECLI:DE:LGBE:2021:0701.525KLS254JS592.20.00, par. 12.

3 Zie bijv. EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*,), par. 321.

4 J. Vervaele, 'Surveillance and criminal investigation: blurring of thresholds and boundaries in the criminal justice system?', in: S. Gutwirth e.a. (red.), *Reloading data protection*, Dordrecht: Springer 2014.

5 Zie bijv. B.W. Schermer, 'Het gebruik van *Big Data* voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *TBS&H* 2017, p. 208; M.F.H. Hirsch Ballin, *Anticipative criminal investigation: theory and counterterrorism practice in the Netherlands and the United States* (diss. Utrecht), Den Haag: Springer 2012, p. 26 en 184.

6 Schermer, *TBS&H* 2017, p. 207-216; I. de Vries, 'Big Data', in: M. den Hengst, T. ten Brink & J. ter Mors (red.), *Informatiegestuurd politiewerk in de praktijk*, Deventer: Vakmedia 2017.

doi: 10.5553/TBSenH/229567002022008002007

personen te verzamelen en te verwerken, vereisen echter een goede regeling in de wet met voldoende waarborgen tegen misbruik, met name vanuit het oogpunt van de bescherming van de *privacy* (art. 8 EVRM). Tal van wetenschappers en beleidsmakers wijzen er op dat het niveau van de waarborgen met betrekking tot grootschalige data-analyse vooralsnog ontoereikend is en dat dit gebrek niet volledig wordt aangepakt door het project Modernisering Strafvordering.[7] In het algemeen hangt het probleem samen met de scheiding in de regeling van het *verzamelen* van gegevens (in het Wetboek van Strafvordering) en de latere *verwerking* van gegevens (voornamelijk genormeerd in de Wet politiegegevens (Wpg)). Het resultaat is dat, terwijl het verzamelen van gegevens in eerste instantie met vrij strikte waarborgen is omgeven, iedere latere verwerking van gegevens geregeld wordt door de minder strenge regels en beginselen van het gegevensbeschermingsrecht. Dit is verrassend en wekt enige verbazing: de inbreuk op de privacy kan namelijk veel groter zijn bij de latere verwerking van gegevens door middel van koppeling en analyse dan bij de enkele vergaring ervan, zoals in gevallen van het uitoefenen van bulkbevoegdheden, wat resulteert in zeer grote hoeveelheden data.

Gelukkig bestaat hiervoor aandacht in de recente jurisprudentie van het Europees Hof voor de Rechten van de Mens ('EHRM' of 'het Hof'). In twee baanbrekende arresten uit mei 2021 heeft de Grote Kamer van het EHRM besloten dat bulkinterceptie van communicatie niet per se onverenigbaar is met de vereisten van artikel 8 lid 2 EVRM.[8] Dit leidde tot kritiek van mensenrechtenwetenschappers die de arresten bekritiseerden voor de 'procedurele' in plaats van 'inhoudelijke' benadering van deze bevoegdheden[9] en de daaruit voortvloeiende 'normalisering van *mass surveillance*'.[10] Niettemin biedt deze procedurele benadering van het Hof, waarbij de nadruk op procedurele waarborgen ligt, belangrijke lessen voor het strafprocesrecht. In de twee arresten maakt het Hof duidelijk dat bulkinterceptie moet worden gezien als een proces dat een gedetailleerde regulering van alle verwerkingsfasen vereist: te weten de verzameling, de selectie, de analyse en het gebruik (waaronder het delen) van de data. In deze korte bijdrage stel ik daarom de vraag: wat kan de jurisprudentie van het EHRM de wetgever en wetenschappers op het gebied van strafprocesrecht leren over de normering van bulk- en andere soorten bevoegdheden die tot grootschalige data-analyse in strafrechtelijk onderzoek leiden? Hoewel de context van de twee EHRM-zaken anders is – het gaat om inlichtingendiensten en nationale veiligheid – kunnen er toch lessen uit worden getrokken over de soorten en voorbeelden van waarborgen met betrekking tot de differentiatie van verschillende handelingen met dezelfde gegevens in strafrechtelijke onderzoeken.

De bijdrage is als volgt opgebouwd: in paragraaf 2 worden in het kort de kenmerken van bulkbevoegdheden besproken, met de nadruk op bulk-hacking zoals die in de EncroChat-zaak plaatsvond. Daarna volgt een beschrijving van de normering van bulkinterceptie van communicatie in de twee bovengenoemde zaken van het EHRM, waarbij eerst de reikwijdte van de analyse in deze bijdrage afgebakend wordt. In paragraaf 3.1 wordt de nieuwe eis van '*end-to-end*' waarborgen voor bulkinterceptie besproken. In de daaropvolgende paragraaf wordt de nieuwe reeks minimumwaarborgen voor bulkinterceptie van communicatie beschreven. Tevens wordt besproken hoe dit als een verschuiving van de focus in de EHRM-toets kan worden gezien: van duidelijke informatie in de machtiging (betreffende de aanvankelijke afbakening van de personen en gegevens) naar de verwerkingsfasen van het bulkinterceptieproces (de selectie, analyse en het gebruik van gegevens). Tot slot wordt er een aantal inzichten uit deze twee arresten besproken voor de normering van bulk- en andere soorten bevoegdheden die tot grootschalige data-analyse in strafrechtelijk onderzoek leiden.

2. Bulk-hacking en bulkinterceptie als soorten bulkbevoegdheden

Zoals vermeld, is de EncroChat-hack een voorbeeld van bulk-hacking. Het gaat om een soort bulkbevoegdheid waarbij digitale technologieën worden gebruikt die gegevens verzamelen, analyseren en/of genereren over zeer grote en grotendeels willekeurige groepen mensen, teneinde nog onbekende personen te identificeren die van belang zijn voor de opsporingsdiensten.[11] Bulkbevoegdheden werken daarom op basis van het principe '*gather in bulk, access in detail*'.[12]

De drie hoofdkenmerken van bulkbevoegdheden zijn: (1) het niet-gerichte karakter van de bevoegdheid, zowel wat betreft de personen op wie de maatregel betrekking heeft als de gegevens die worden verzameld; (2) het ontbreken van – of een zeer lage standaard van – een rede-

7 Zie bijv. Wetenschappelijke Raad voor het Regeringsbeleid, *Big data in een vrije en veilige samenleving*, Amsterdam: Amsterdam University Press 2016, p. 27; Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, 2018 (Commissie-Koops), p. 24-25; Schermer, *TBS&H* 2017, p. 207.

8 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*); EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208, nr. 35252/08 (*Centrum för rättvisa t. Zweden)*.

9 De nadruk ligt hier niet op de inhoudelijke rechtmatigheid van *surveillance regimes*, maar op procedurele waarborgen, uitgaande van hun evenredigheid, functionaliteit en doeltreffendheid; zie M. Zalnieriute, 'Procedural fetishism and mass surveillance under the ECHR', *Verfassungsblog* 2 juni 2021.

10 M. Milanović, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa', *EJIL: Talk!* 26 mei 2021; N. Ní Loideáin, 'Bulk surveillance: Europe's recent landmark judgements', *Digital Freedom Fund Blog* 5 juli 2021.

11 Cf. R. Clarke en G. Greenleaf, 'Dataveillance Regulation: A Research Framework', *Journal of Law, Information and Science* (25) 2017, afl. 1.

12 P. Bernal, 'Data gathering, surveillance and human rights: recasting the debate', *Journal of cyber policy* (1) 2016, afl. 2, p. 246.

lijk vermoeden dat een misdrijf is of zal worden gepleegd, alsmede het ontbreken van een verdachte of een groep verdachten; en (3) het resulteren in een enorme hoeveelheid gegevens die in tal van toekomstige onderzoeken zullen worden gebruikt. In de EncroChat-zaak bijvoorbeeld lijkt de verdenking te zijn gebaseerd op een zeer algemene veronderstelling dat het enkele gebruik van een EncroChat-cryptotelefoon wijst op samenzweerderig gedrag om misdrijven te plegen en te verdoezelen.[13] Dit werd verondersteld omdat de EncroChat-telefoons een zeer ingewikkeld en duur beveiligingssysteem hebben en omdat ze in eerdere Franse strafrechtelijke onderzoeken zijn aangetroffen.[14] Er waren echter geen concrete vaststellingen dat deze algemene veronderstelling inderdaad opging in het specifieke geval van alle gebruikers van gehackte EncroChat-telefoons.[15]

Een bekender voorbeeld van een bulkbevoegdheid is bulkinterceptie van communicatie. Bulkinterceptie en bulk-hacking zijn duidelijk twee verschillende bevoegdheden. Bulk-hacking – ook wel het 'Zwitserse zakmes' van bevoegdheden genoemd[16] – omvat een veel breder scala aan functionaliteiten dan bulkinterceptie, zoals het kopiëren van opgeslagen gegevens, het aanzetten van de microfoon of camera en het wissen van gegevens. Bulkinterceptie van communicatie door inlichtingendiensten vindt op nog grotere schaal plaats dan bulk-hacking, aangezien het gericht is op communicatiedragers zelf en niet op de computers waarmee de communicatie werd verzonden of ontvangen. Niettemin hebben beide de drie bovengenoemde hoofdkenmerken van bulkbevoegdheden gemeen en zijn daarmee voldoende vergelijkbaar.

13 Zie bijv. B. Derin en T. Singelnstein, 'Verwendung und verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat)', *NStZ* 2021, p. 452.

14 Sinds 2016 zijn cryptotelefoons ook in Nederland in toenemende mate aangetroffen bij aangehouden verdachten.

15 Op basis van een evaluatie van het gebruik van EncroChat-telefoons in Frankrijk vanaf 12 juni 2020, gebruikte 67,3% van de gebruikers de cryptotelefoons voor criminele doeleinden (317 van de 471). Voor de overige 32,7% van de telefoons kon niet worden vastgesteld dat zij voor criminele doeleinden waren gebruikt en dat er dus mogelijk onschuldige gebruikers bij betrokken waren (zie Landgericht Berlin, 1 juli 2020, ECLI:DE:LGBE:2021:0701.525KLS254JS592.20.00, par. 10). Een nauwkeuriger percentage van 'onschuldig gebruik' is echter moeilijk vast te stellen. Voor een bespreking van de eisen inzake redelijke verdenking in de context van digitale technologieën (in het bijzonder in de context van *predictive policing*) zie R.A. Hoving, 'Verdacht door een algoritme. Kan predictive policing leiden tot een redelijke verdenking?', *DD* 2019/41.

16 I. Škorvánek, B.J. Koops, B.C. Newell en A. Roberts, '"My computer is my castle": new privacy frameworks to regulate police hacking', *BYU Law Review* 2019, afl. 4, p. 1008.

3. De normering van de bulkbevoegdheden: een EHRM-perspectief

In mei 2021 heeft de Grote Kamer van het EHRM twee baanbrekende arresten gewezen over bulkinterceptie door inlichtingendiensten in het kader van de nationale veiligheid: *Big Brother Watch e.a. tegen het Verenigd Koninkrijk* en *Centrum för rättvisa tegen Zweden*. Omdat deze twee arresten betrekking hebben op inlichtingendiensten en nationale veiligheid, moeten de inzichten die eruit voortvloeien slechts worden gezien als een indicatie van het soort waarborgen die vereist kunnen worden in de context van bulkbevoegdheden en grootschalige data-analyse in strafrechtelijk onderzoek (mits het EHRM de mogelijkheid om dergelijke bevoegdheden in strafrechtelijke onderzoeken te gebruiken niet zou uitsluiten).[17]

In de twee bovengenoemde arresten heeft het Hof toch vrij duidelijk gesteld dat '*bulk interception may [also] be used to investigate certain serious crimes*'.[18] Het EHRM heeft er echter herhaaldelijk op gewezen dat de staten met betrekking tot de nationale veiligheid over een ruime *margin of appreciation* beschikken om te bepalen welke soorten maatregelen hiervoor nodig zijn.[19] In de context van strafrechtelijk onderzoek door de politie is de margin of appreciation over het algemeen wat meer beperkt, zodat er waarschijnlijk een strengere toetsing aan lid 2 van artikel 8 EVRM zal moeten plaatsvinden.[20] In de conclusie wordt hiermee rekening gehouden bij de bespreking van de lessen die uit het EHRM kunnen worden getrokken.

3.1 Het proces van bulkinterceptie en de eis van 'end-to-end-waarborgen'

Tot nu toe paste het EHRM de zes minimumwaarborgen,[21] die in de jaren negentig zijn ontwikkeld voor ge-

17 Dit is zeker een vraag die het EHRM zal moeten beantwoorden en er zijn goede argumenten tegen het gebruik van bulkbevoegdheden, zoals bulkhacking, in strafrechtelijk onderzoek. Zie bijv. M. Gutheil e.a., *Legal Frameworks for Hacking by Law Enforcement: study for the LIBE Committee*, 2017.

18 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*,), par. 345; EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208, nr. 35252/08 (*Centrum för rättvisa t. Zweden)*, par. 259.

19 Zie de EHRM-jurisprudentie en discussie in D. Spielmann, 'Allowing the Right Margin: The European Court of Human Rights and the National Margin of Appreciation Doctrine: Waiver or Subsidiarity of European Review', *Cambridge Yearbook of European Legal Studies* 14 (381), 2011-2012.

20 Cf. N. Ní Loideain, 'The approach of the European Court of Human Rights to the interception of communications', in: *EU data privacy law and serious crime: data retention and policymaking*, Oxford: Oxford University Press (forthcoming), p. 61-2 (toegankelijk via www.papers.ssrn.com/sol3/papers.cfm?abstract_id=3699386).

21 De zes minimumwaarborgen voor de gerichte interceptie van communicatie zijn: '(1) *the nature of offences which may give rise to an interception order*; (2) *a definition of the categories of people liable to have their communications intercepted*; (3) *a limit on the duration of interception*; (4) *the procedure to be followed for examining, using and storing the data obtained*; (5) *the precautions to be taken when communicating the data to other parties*; *and* (6) *the circumstances in which intercepted data may or must be erased or destroyed*'

doi: 10.5553/TBSenH/229567002022008002007

richte interceptie van communicatie (uitgevoerd door de politie), routinematig toe op de bulkinterceptie van inlichtingendiensten. Deze waarborgen voor gerichte interceptie vereisen onder meer 'een omschrijving van de categorieën personen wiens communicatie kan worden afgetapt' en een 'redelijke verdenking', eisen waaraan bulkbevoegdheden per definitie niet kunnen voldoen. Deze aanpak kreeg kritiek – zelfs door rechters van het EHRM zelf – omdat er geen rekening wordt gehouden met de '*technological sea change*' die het digitale tijdperk heeft meegebracht.[22] In de zaken *Big Brother Watch* en *Centrum för rättvisa* brak het Hof uiteindelijk met deze oude benadering door te stellen dat sommige van de bestaande vereisten eenvoudigweg niet geschikt zijn voor bulkinterceptie.[23] Het EHRM ontwierp daarop een nieuwe benadering voor de regulering van bulkbevoegdheden.

In de twee zaken erkent het Hof voor het eerst expliciet dat bulkinterceptie verenigbaar kan zijn met de vereisten van artikel 8 lid 2 EVRM.[24] Het Hof merkt echter op: terwijl de *keuze* van het systeem binnen een ruime margin of appreciation valt, valt de *werking* (*operation*) van een dergelijk systeem binnen een engere marge, die een uitgebreid en vernieuwd geheel van waarborgen in de wet vereist.[25] Om de regeling verenigbaar te maken met het recht op eerbiediging van het privéleven, moet bulkinterceptie onderworpen zijn aan – in de woorden van het Hof – 'end-to-end-waarborgen'.[26] Hiermee verwijst het Hof naar de alomvattende bescherming die door 'end-to-end-encryptie' wordt geboden.[27]

Om het risico van misbruik van zo'n indringende bevoegdheid tot een minimum te beperken, is in elke fase van het *proces* van bulkinterceptie een beoordeling van de noodzaak en de proportionaliteit van de maatregelen vereist.[28] Het Hof merkt hierbij specifiek op dat bulkinterceptie – net als andere soorten bulkbevoegdheden – een geleidelijk proces is, waarbij er vier hoofdfasen kunnen worden onderscheiden:

1. *verzameling*: het aftappen en aanvankelijk bewaren van alle communicatie en metadata;
2. *selectie*: de toepassing van specifieke selectiecriteria (*selectors*; bijv. complexe zoekopdrachten, eenvoudige zoektermen, e-mailadressen, IMEI-nummers) op de bewaarde communicatie en verkeersgegevens, wat tot de geselecteerde (of secundaire) dataset leidt;
3. *analyse*: het onderzoek van de geselecteerde dataset; en
4. *gebruik*: verdere bewaring van gegevens en het gebruik van het 'eindproduct', met inbegrip van het delen van gegevens met derden.[29]

De bulkinterceptiebevoegdheid moet dus worden gezien als een proces dat waarborgen vereist met betrekking tot alle onderdelen ervan. Dit is een waardevol inzicht, vooral voor de normering van digitale bevoegdheden, die niet mag worden geleid door een simplistisch onderscheid tussen het *verzamelen* en het *verwerken* van gegevens (en die gereguleerd worden door twee zeer verschillende soorten wetten). Volgens het Hof neemt de mate van de inmenging in de persoonlijke levenssfeer toe naarmate het proces van bulkinterceptie vordert.[30] Met andere woorden: de verwerking van de geselecteerde gegevens (vanaf fase 2) is veel indringender dan de aanvankelijke verzameling van een grote hoeveelheid data en de tijdelijke bewaring ervan (in fase 1). Dat komt doordat fase 2 begint met het daadwerkelijk uitlichten van personen (*targeted*) door de toepassing van selectiecriteria (de meeste data die in fase 1 zijn verzameld, zijn daarom niet doorzocht).[31] De EHRM-toets is derhalve toegespitst op de laatste drie fasen van het proces van bulkinterceptie: de selectie en verwerking van gegevens en het gebruik van het resultaat.

3.2 Een verschuiving in de EHRM-toets: focus op de verwerkingsfasen van het proces van bulkinterceptie

In overeenstemming met deze focus van de EHRM-toets op de verwerking van de grote hoeveelheid verzamelde gegevens, heeft het Hof de oude zes minimumwaarbor-

(EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 335).

22 'Opinion of Judges Koskelo and Turković', par. 308 in EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*). Zie ook K. Hughes, 'Mass surveillance and the European Court of Human Rights', *European Human Rights Law Review* 6, 2018.

23 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 348.

24 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 347.

25 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 347.

26 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 350.

27 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 350.

28 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 350. De eis van end-to-end-waarborgen lijkt ook in te houden dat het gebrek aan waarborgen in een van deze fasen niet kan worden hersteld door waarborgen in een andere fase, of dat dit alleen met grote moeite kan worden bereikt. Dit is een aanzienlijk strengere aanpak dan de vorige, waarbij het ontbreken van waarborgen in één stadium van het proces kan worden verholpen door waarborgen in een ander (gewoonlijk later) stadium (zie bijv., EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*)).

29 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 325.

30 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 330.

31 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 330.

gen vervangen door een vernieuwde en uitgebreide lijst van waarborgen:

1. de gronden waarop bulkinterceptie kan worden toegestaan;
2. de omstandigheden waarin de communicatie van een persoon mag worden afgetapt;
3. de procedure die moet worden gevolgd voor het verlenen van de machtiging;
4. de procedures die moeten worden gevolgd voor het selecteren, analyseren en gebruiken van het onderschepte materiaal;
5. de voorzorgsmaatregelen die moeten worden genomen bij het doorgeven van het materiaal aan andere partijen;
6. de beperkingen inzake de duur van het aftappen, de opslag van de afgetapte gegevens en de omstandigheden waaronder de gegevens moeten worden gewist en vernietigd;
7. de procedures en modaliteiten voor het toezicht door een onafhankelijke autoriteit op de naleving van bovengenoemde waarborgen en haar bevoegdheden om bij niet-naleving op te treden; en
8. de procedures voor een onafhankelijke *ex post facto* toetsing van die naleving en de bevoegdheden van de bevoegde instantie om gevallen van niet-naleving aan te pakken.[32]

Uit deze nieuwe lijst van waarborgen en de beoordeling van het EHRM in de twee zaken blijkt dat het Hof zich zeer soepel opstelt met betrekking tot de eerste twee vereisten. De gronden voor toestemming en de omstandigheden waaronder iemands communicatie mag worden afgetapt, kunnen in de machtiging op zeer ruime wijze worden geformuleerd.[33] De reden hiervoor is duidelijk:

> '*[i]n a bulk interception regime the circumstances in which communications might be intercepted will be very broad, as it is the communications bearers that are targeted … The circumstances in which communications may be examined will be narrower, but compared to targeted interception this category will still be relatively wide, since bulk interception may be used for a more varied range of purposes, and communications may be selected for examination by reference to factors other than the identity of the sender or recipient*.'[34]

In plaats daarvan richt de aandacht van het Hof zich op twee andere soorten waarborgen: toezicht op en ex post toetsing van de bevoegdheid (waarborgen 7-8) en procedurele voorschriften betreffende de verwerking van gegevens (waarborgen 4-6).

De focus op deze waarborgen kan worden gezien als een verschuiving in de EHRM-toets. Terwijl het EHRM voorheen in zijn jurisprudentie over *secret surveillance* de beginselen van voorzienbaarheid en noodzakelijkheid (aangezien de twee vaak samen beschouwd worden[35]) traditioneel koppelde aan duidelijke informatie in de machtiging (betreffende de initiële afbakening van personen en gegevens),[36] richt het Hof zijn aandacht nu in de eerste plaats op de regulering van de verwerkingsfasen van het bulkinterceptieproces.[37] Met andere woorden: het Hof staat nu een zeer ruime gegevensvergaring toe, maar eist vervolgens tamelijk gedetailleerde procedures en regels voor de analyse, bewaring en het delen van die gegevens, versterkt met ruime bevoegdheden voor het toezicht en de controle daarop.[38]

Helemaal nieuw is deze benadering natuurlijk niet. Het EHRM heeft in oudere arresten, vooral over databanken, reeds gewezen op het belang van waarborgen voor de verwerking van gegevens, zoals bewaartermijnen, beperkte toegang tot de data en veilige opslag ervan.[39] In de twee zaken betreffende bulkinterceptie heeft het Hof echter voor het eerst benadrukt hoe belangrijk het is dat het gehele proces van gegevensverwerking, wanneer geavanceerde opsporingstechnieken worden ingezet, adequaat is gereguleerd. Met uitzondering van de arresten van de lagere kamer in diezelfde twee zaken uit 2018,[40] is dit ook de eerste keer dat het Hof de regeling bespreekt die het nodig acht voor het delen van gegevens tussen (buitenlandse) instellingen, een belangrijk onderwerp

32 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 361; EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208, nr. 35252/08 (*Centrum för rättvisa t. Zweden*), par. 284.

33 Bijvoorbeeld interceptie voor 'doeleinden van nationale veiligheid' van die 'dragers die hoogstwaarschijnlijk internationale communicatie overbrengen' (EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 371 en 376).

34 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208, nr. 35252/08 (*Centrum för rättvisa t. Zweden*), par. 289.

35 Zie bijv. EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306, nr. 47143/016 (*Roman Zakharov t. Rusland*), par. 236: '*In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements (see Kennedy, cited above, § 155; see also Kvasnica, cited above, § 84).*'

36 Cf. E. Kosta, *Surveilling masses and unveiling human rights: uneasy choices for the Strasbourg Court*, Tilburg: Tilburg University (oratie), 2017, p. 49; N. Ní Loideain, 'The approach of the European Court of Human Rights to the interception of communications', in: *EU data privacy law and serious crime: data retention and policymaking*, Oxford: Oxford University Press (forthcoming), p. 52. Zie EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306, nr. 47143/016 (*Roman Zakharov t. Rusland*) en EHRM 12 januari 2016, ECLI:CE:ECHR:2016:0112JUD003713814, nr. 37138/14 (*Szabo en Vissy t. Hongarije*).

37 Zie ook V. Rusinova, 'Privacy and the legislation of mass surveillance: in search of a second wind for international human rights law', *The International Journal of Human Rights Law*, 2021, p. 6.

38 Cf. M. Hagens en J.J. Oerlemans, 'Big Brother Watch e.a. t. VK (EHRM, 58170/13 e.a.) en Centrum för Rättvisa t. Zweden (EHRM, 35252/08) – Legitimering bulkinterceptie', *European Human Rights Cases Updates* (13 september 2021).

39 Zie bijv. EHRM 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204, nr. 30562/04 en 30566/04 (*S. en Marper t. Verenigd Koninkrijk*), par. 99 en 103.

40 EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*).

doi: 10.5553/TBSenH/229567002022008002007

in de context van grootschalige data-analyse.[41]

Het Hof geeft geen concrete lijst van de procedures en regels met betrekking tot de uitgebreide lijst van waarborgen die in de wet moeten worden opgenomen. Er worden wel verschillende voorbeelden besproken in de beoordeling van de wettelijke kaders voor bulkinterceptie in Engeland en Zweden. Deze voorbeelden zijn onder meer: procedures betreffende de keuze en het gebruik van selectiecriteria; toegang van gemachtigde personen tot de geselecteerde dataset (resulterend uit fase 2 van het bulkinterceptieproces); de duur en de reikwijdte van die toegang; verplichte registratie en gedetailleerde verslagen betreffende elke stap in het bulkinterceptieproces; regelmatige audits; veilige opslag van de gegevens; de duur van de interceptie en de voorwaarden voor verlenging; maximale bewaarperioden en regels inzake de vernietiging van gegevens voor verschillende categorieën materiaal, die de aard en de indringendheid ervan weerspiegelen (bijvoorbeeld voor onderzoek geselecteerde of niet geselecteerde gegevens en verschoningsgerechtigde communicatie); geautomatiseerde verwijdering van gegevens na het verstrijken van de bewaringstermijn; en een beoordeling van de noodzakelijkheid en evenredigheid van het delen van de (*ruwe* of verwerkte) gegevens of inlichtingen.[42]

Een bijzonder belangrijke rol speelt de keuze van de selectiecriteria die het Hof ook bespreekt in verband met de machtiging.[43] Het gebruik van selectiecriteria wordt namelijk gezien als '*one of the most important steps in the bulk interception process, as this is the point at which the communications of a particular individual may be targeted by the intelligence service*'.[44] Als zodanig moeten alle door analisten verrichte zoekopdrachten in de verzamelde gegevens (fase 3 van het bulkinterceptieproces) worden geregistreerd, met inbegrip van de gebruikte selectiecriteria, het tijdstip, de naam van de analist, de motivering van de zoekopdracht, de gedetailleerde taakomschrijving en de reden voor de zoekopdracht.[45] Bovendien vereisen 'krachtige selectiecriteria' (*strong selectors*; bijv. email- of MAC-adressen, IMEI-nummers en andere *unique identifiers*) strengere waarborgen, zoals een voorafgaande interne machtiging.[46]

Gezien de steeds grotere rol van het delen van gegevens tussen (buitenlandse) inlichtingendiensten, maar ook andere rechtshandhavingsinstanties (zoals ook te zien is in de EncroChat-zaak), is het jammer dat de Grote Kamer de overwegingen op dit punt van de Eerste Kamer in het *Big Brother Watch*-arrest uit 2018 niet heeft gevolgd en verder uitgewerkt. De Eerste Kamer erkende namelijk expliciet het gevaar voor het omzeilen van binnenlandse waarborgen en beperkingen door het delen van inlichtingengegevens tussen buitenlandse inlichtingendiensten:

> '*[A]s the Venice Commission noted, as States could use intelligence sharing to circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations, a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques*.'[47]

Terwijl de Grote Kamer in de *Centrum för rättvisa*-zaak wel een schending constateert met betrekking tot het regime voor het delen van gegevens tussen inlichtingendiensten,[48] hield de beoordeling geen rekening met het gevaar van omzeiling van binnenlandse regels.

Ten slotte moet het toezicht op het gehele proces van bulkinterceptie onafhankelijk en effectief zijn.[49] Het toezicht wordt niet alleen – of vooral – gericht op de beoordeling van de noodzaak en de evenredigheid van de machtiging (met bijzondere aandacht voor de keuze van de selectiecriteria), die hoe dan ook beperkt zal zijn gezien het gebrek aan detail in de machtiging. Integendeel, het toezicht moet worden toegespitst op de procedures voor toegang, bewaring, opslag, vernietiging en het delen van het materiaal.[50] Om een dergelijke beoordeling te kunnen maken, moet de toezichthoudende instantie ook toegang hebben tot de dossiers die over elke

41 B. van der Sloot en E. Kosta, 'Big Brother Watch and others v. UK: lesson from the latest Strasbourg ruling on bulk surveillance', *European Data Protection Law* 2019, afl. 2, p. 259.

42 Zie EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 387, 388, 390, 400, 402; EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208, nr. 35252/08 (*Centrum för rättvisa t. Zweden)*, par. 309, 311, 312, 326, 342, 343.

43 Selectiecriteria (of ten minste de categorieën van de selectiecriteria) moeten in de machtiging worden gespecificeerd; EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 382; EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208, nr. 35252/08 (*Centrum för rättvisa t. Zweden)*, par. 299-300.

44 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 353.

45 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208, nr. 35252/08 (*Centrum för rättvisa t. Zweden)*, par. 309.

46 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 355 en 382.

47 EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 423-424. Zie ook B. van der Sloot en E. Kosta, *EDPL* 2019/2, p. 259.

48 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208, nr. 35252/08 (*Centrum för rättvisa t. Zweden)*, par. 318 en 330.

49 Het Hof van Justitie van de Europese Unie heeft onlangs ook een uitspraak gedaan over het toezicht op de bewaring van gegevens; zie HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur*). Zie ook 'Toepassing Prokuratuur-arrest: onherstelbaar vormverzuim doordat is gehandeld in strijd met het Unierecht', *Tijdschrift Bijzonder Strafrecht & Handhaving* 1 september 2021, www.bijzonderstrafrecht.nl/home/toepassing-prokuratuur-arrest-onherstelbaar-vormverzuim-doordat-is-gehandeld-in-strijd-met-het-unierecht.

50 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 412.

fase van het interceptieproces worden bijgehouden.[51] De ex post toetsing moet ook een effectief rechtsmiddel zijn dat beschikbaar wordt voor iedereen die vermoedt dat zijn of haar communicatie is afgetapt, en dat de toezichthoudende instantie ruime bevoegdheden heeft, zoals het toekennen van schadevergoeding, het vernietigen van de machtiging en de verzamelde gegevens of eindresultaten.[52]

4. Tot slot: lessen van het EHRM voor het strafprocesrecht

In deze bijdrage heb ik twee baanbrekende arresten van het EHRM onder de loep genomen met de bedoeling er lessen uit te trekken voor de normering van bulk- en andere bevoegdheden die leiden tot grootschalige data-analyse in strafrechtelijk onderzoek. Hoewel de context van de twee arresten anders is – ze betreffen nationale veiligheid in plaats van strafrechtelijk onderzoek – is dit een waardevolle vergelijking, omdat het Hof een nieuwe benadering heeft toegepast bij de beoordeling van de bulkinterceptiebevoegdheid en de verenigbaarheid daarvan met de vereisten van artikel 8 lid 2 EVRM. Lag het zwaartepunt van de beoordeling voorheen bij duidelijke informatie in de machtiging (afbakening van personen en gegevens en een redelijk vermoeden van strafbare feiten), nu ligt het zwaartepunt primair bij de verwerkingsfasen van het proces van bulkinterceptie, waarvoor een duidelijke en gedetailleerde regeling van alle fasen vereist is: verzameling, selectie, analyse en gebruik. Uit deze discussie kunnen een aantal lessen voor het strafprocesrecht worden getrokken. De punten die het EHRM benadrukt in de twee besproken zaken over bulkinterceptie, sluiten ook goed aan bij de bestaande kritiek op de normering van digitale opsporingsbevoegdheden in het Nederlandse strafprocesrecht.

Ten eerste moeten bulkbevoegdheden worden gezien als een proces, dat zowel het verzamelen van gegevens als de verschillende fasen van gegevensverwerking en het gebruik van het eindresultaat omvat. De regulering van zulke bevoegdheden moet derhalve al deze fasen omvatten, waarbij in de latere fasen van de verwerking – waar een grotere inbreuk op de privacy plaatsvindt – steeds meer waarborgen in de wet moeten worden ingebouwd. Deze les geldt eigenlijk voor de regulering van digitale onderzoeksbevoegdheden in het algemeen, aangezien deze vaak (of zelfs doorgans) leiden tot grootschalige data-analyse in strafrechtelijke onderzoeken. Hoewel de mate van de inbreuk reeds bepalend is voor de striktheid van de waarborgen, lijken de Nederlandse strafrechters toch onvoldoende rekening te houden met het volledige proces van data-analyse bij het gebruik van digitale opsporingsbevoegdheden.[53] In plaats daarvan wordt de mate van inbreuk op de persoonlijke levenssfeer meestal pas bekeken bij de allereerste stap: bij het vergaren van gegevens.[54] Indien een bepaalde bevoegdheid het mogelijk maakt eenmalig gegevens te verzamelen die voor zichzelf niet bijzonder privacygevoelig zijn (bijvoorbeeld bij het gebruik van IMSI-*catchers* en stille SMS), wordt vrij snel beoordeeld dat de privacy-inbreuk gering is.[55] Deze benadering gaat echter voorbij aan het feit dat het opzetten van grote databanken en de daaropvolgende verwerking van de gegevens door geavanceerde technologieën in verschillende strafrechtelijke onderzoeken, een steeds gebruikelijker praktijk in Nederland is.[56] De latere verwerking en het latere gebruik van data vragen dus om een eigen toets aan artikel 8 EVRM.

Ten tweede kan uit de arresten worden afgeleid dat het EHRM vrij gedetailleerde procedures en specifieke regels eist met betrekking tot de selectie, analyse en het gebruik van de gegevens (bijv. maximale bewaringstermijnen voor bepaalde soorten gegevens, geautomatiseerde verwijdering van gegevens na het verstrijken van de bewaringstermijn). Dit zou kunnen betekenen dat de zeer algemene en abstracte gegevensbeschermingsregels en -beginselen van de Wpg onvoldoende garanties bieden in het kader van artikel 8 EVRM. De hoeksteen van gegevensbeschermingsrecht wordt namelijk gevormd door de beginselen van eerlijke verwerking (*fair processing principles*), zoals specificatie- en minimalisatiebeginselen.[57] Volgens deze beginselen moeten persoonsgegevens voor bepaalde, uitdrukkelijk omschreven en legitieme doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt.[58] De gegevens moeten ook toereikend, ter zake dienend en niet bovenmatig zijn ten opzichte

51 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 412.

52 De toetsing moet zoveel mogelijk een contradictoir proces garanderen, hetgeen ook betekent dat de beslissingen gemotiveerd en juridisch bindend moeten zijn (EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208, nr. 35252/08 (*Centrum för rättvisa t. Zweden*), par. 361-2); EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, nr. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), par. 413.

53 Cf. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van Opsporingsbevoegdheden in Een Digitale Omgeving* (2018), p. 24-26.

54 Zie bijv. Hoge Raad, 1 juli 2014, ECLI:NL:HR:2014:1563; Hoge Raad, 1 juli 2014, ECLI:NL:HR:2014:1562; Hoge Raad, 1 juli 2014, ECLI:NL:HR:2014:1569.

55 Zie bijv. Hoge Raad, 1 juli 2014, ECLI:NL:HR:2014:1563; Hoge Raad, 1 juli 2014, ECLI:NL:HR:2014:1562; Hoge Raad, 1 juli 2014, ECLI:NL:HR:2014:1569.

56 Over de toepassing van gezichtsherkenningstechnologie in enorme databanken, die foto's bevatten van personen die niet (langer) van een misdrijf worden verdacht, zie bijv. 'Antwoorden Kamervragen over Het Bericht "Gezichtendatabase van Politie Bevat Foto's van 1,3 Miljoen Mensen"', *Ministerie van Justitie en Veiligheid* 10 september 2019, p. 3.

57 Art. 4 Richtlijn 2016/680.

58 Voor een nadere beschouwing van gegevensbeschermingsrecht zie L. Stevens, M.F.H. Hirsch Ballin, M. Galič e.a., 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling', *TBS&H* 2021, p. 234-245.

doi: 10.5553/TBSenH/229567002022008002007

van de doeleinden waarvoor zij worden verwerkt.[59] Deze beginselen worden echter niet verduidelijkt of geconcretiseerd in de bepalingen van de Wpg, wat ze moeilijk te operationaliseren maakt.[60] Ze sluiten ook niet goed aan op de opsporingspraktijk. Volgens het WODC-onderzoek over de verwerking van politiegegevens lijken gegevens niet makkelijk in te delen in een van de weinige categorieën met bijbehorende verwerkingsregimes in de Wpg (bijv. het wettelijk onderscheid tussen 'dagelijkse politietaken' in art. 8 en 'onderzoek' in art. 9 Wpg).[61] Voor politiemedewerkers is het ook nog vaak onduidelijk of ze gegevens mogen verstrekken en onder welke voorwaarden.[62] Hieruit kan daarom worden geconcludeerd dat voor indringende onderzoeksbevoegdheden, waaronder zeker bulkbevoegdheden, eigen en gedetailleerde regels inzake gegevensbescherming zouden moeten gelden.

Dit sluit aan bij de derde les met betrekking tot toezicht en ex post toetsing die we uit EHRM-jurisprudentie kunnen trekken. Personen wier gegevens worden verwerkt, die van mening zijn dat de verwerking van hun gegevens volgens de Wpg niet rechtmatig of rechtvaardig is, kunnen een klacht indienen bij de Autoriteit Persoonsgegevens (AP). Aangezien mensen niet op de hoogte zijn van de overheidspraktijken met betrekking tot gegevensverwerking voor opsporingsdoelen (en dat hun rechten op basis van de Wpg ook kunnen worden beperkt als dat niet in het belang van het onderzoek is),[63] wordt de mogelijkheid om zich op dit recht te beroepen ernstig beperkt. In de praktijk is dan ook zeer weinig gebruik gemaakt van de procedurele mechanismen die de Wpg biedt.[64] De controle op de naleving van de Wpg is daarom in belangrijke mate afhankelijk van de *proactieve* uitoefening van toezichtsbevoegdheden door de AP. Onder de Wpg heeft de AP echter veel minder corrigerende en toezichthoudende bevoegdheden dan onder de AVG. Zij heeft bijvoorbeeld geen bevoegdheid om verwerkingen stil te leggen of onrechtmatig verwerkte gegevens zelf te verwijderen.[65] En dat is kennelijk niet in lijn met de strenge vereisten van het EHRM met betrekking tot ex post controle die uit de twee nieuwe uitspraken voortvloeien. Om ervoor te zorgen dat de door het EHRM vereiste bescherming niet louter illusoir zou zijn, zouden de bevoegdheden (maar zeker ook de capaciteiten) van de AP moeten worden versterkt. Een andere mogelijkheid zou zijn om de gedetailleerde regels inzake gegevensbescherming in het Wetboek van Strafvordering zelf op te nemen, zodat het toezicht ook primair bij de rechter-commissaris en uiteindelijk de zittingsrechter zou komen te liggen.[66]

Tot slot: er moeten ook duidelijke regels met passende waarborgen komen voor het delen van data tussen buitenlandse rechtshandhavingsinstanties, om te voorkomen dat binnenlandse wettelijke beperkingen kunnen worden omzeild. Dit blijkt onder andere uit de discussie over het interstatelijke vertrouwensbeginsel in verband met de Franse EncroChat-operatie en de talrijke Nederlandse strafzaken die daaruit zijn voortgevloeid, zoals besproken door Schermer en Oerlemans in een andere bijdrage aan dit speciale nummer van het *Tijdschrift voor Bijzonder Strafrecht & Handhaving*. Helaas heeft het EHRM nagelaten in de twee besproken zaken dergelijke regels te ontwikkelen, ondanks dat hier wel degelijk behoefte aan is.

59 Art. 4 Richtlijn 2016/680.

60 Zie H. Winter e.a., *De verwerking van politiegegevens in vijf Europese landen*, Den Haag: WODC, 2020. Zie ook Stevens, Hirsch Ballin, Galič e.a. *TBS&H* 2021, p. 234-245.

61 Winter 2020, p. 15.

62 Winter 2020, p. 15.

63 Bijv. art. 27, lid 1, onder b) Wpg; art. 13 t/m 16 Richtlijn 2016/680.

64 B. Custers en M. Leiser, 'Persoonsgegevens in het strafrecht: weeffouten in EU-Richtlijn 2016/680 leiden tot praktische problemen', *NJB* 2019/2107.

65 P. de Hert en J. Sajfert, 'The role of data protection authorities in supervising police and criminal justice authorities processing personal data', in: C. Brière & A. Weyembergh (red.), *The needed balances in EU Criminal Law: past, present and future*, London: Hart 2018, p. 251-252; zie ook de discussie in Stevens, Hirsch Ballin, Galič e.a. *TBS&H* 2021, p. 240-241.

66 Schermer *TBS&H* 2017, p. 214.

doi: 10.5553/TBSenH/229567002022008002007