Recente uitspraken van het EHRM en de totstandkoming van Conventie 108+ in relatie tot het stelsel van toezicht op inlichtingen- en veiligheidsdiensten (BZK interne analyse)

Inleiding

Gevraagd is om een juridische analyse van recente jurisprudentie van het Europese Hof voor de Rechten van de Mens (verder: EHRM) in relatie tot het stelsel van toezicht op inlichtingen- en veiligheidsdiensten. In het verlengde daarvan is dit stelsel eveneens bezien tegen de achtergrond van de totstandkoming van het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (beter bekend onder Conventie 108+ of C-108+). Tot besluit worden enkele observaties gedaan die van nut kunnen zijn bij het maken van (beleids)keuzes ten aanzien van de wettelijke inrichting van het stelsel van toezicht.

Omdat de geanalyseerde uitspraken van het EHRM buitengewoon omvangrijk zijn, is besloten het document waarin puntsgewijs verslag wordt gedaan van de analyse hiervan afzonderlijk te presenteren (bijlage). In deze notitie zullen alleen de hoofdlijnen aan de orde komen.

Twee recente uitspraken van het EHRM

In bijgevoegde analyse van de twee actuele uitspraken van het EHRM inzake Big Brother Watch e.a. tegen het VK en Centrum för Rättvissa tegen Zweden is bezien welke eisen het EHRM thans stelt met betrekking tot stelsels van bulkinterceptie van communicatie (inhoud en gerelateerde verkeersgegevens) om te voldoen aan de eisen die uit artikel 8 EVRM voortvloeien. De thans door het Hof geformuleerde eisen (acht stuks) bouwen voort op de zes eerder door het Hof ontwikkelde eisen, die beter bekend staan als de zogeheten Weber-criteria. Die criteria waren echter primair ontwikkeld in een opsporingscontext en bovendien niet afgestemd op de bijzonderheden die verbonden zijn aan bulkinterceptie. Daarnaast heeft het Hof ook de *bevraging* van buitenlandse diensten (in het Britse stelsel) alsmede de *verstrekking* aan buitenlandse diensten (in het Zweedse stelsel) van geïntercepteerd materiaal in het licht van artikel 8 EVRM beoordeeld. In de Britse zaak is ook ingegaan op artikel 10 EVRM – in casu de bescherming van vertrouwelijk journalistiek materiaal in relatie tot bronbescherming – in de context van bulkinterceptie.

In de analyse is ook bezien wat de gevolgen van beide uitspraken (kunnen) zijn voor het huidige wettelijke kader voor de Nederlandse inlichtingen- en veiligheidsdiensten, de Wiv 2017 (dit betreft de vetgedrukte stukken tekst). De algemene conclusie die kan worden getrokken is, dat de huidige wet nog steeds voldoet aan de eisen van het EVRM en de jurisprudentie van het EHRM, zij het dat op een aantal onderdelen het wel aangewezen wordt geacht de wet aan te passen. Dat betreft:

1. de in artikel 50 van de wet neergelegde regeling inzake selectie op de uit OOG-interceptie verkregen gegevens;
2. (a) de mogelijkheid tot bevraging van buitenlandse diensten om geïntercepteerd materiaal en (b) de daarop toe te passen waarborgen bij (verdere) verwerking;
3. De autorisatie van het kunnen kennisnemen (selectie) c.q. de voortdurende opslag en onderzoek van vertrouwelijk journalistiek materiaal (in geval van bijvangst) waaruit de bron van een journalist kan worden afgeleid.

Waar het gaat om punt 1 verzet de huidige wet zich er niet tegen dat in verzoeken om toestemming tot selectie in aanvulling op hetgeen nu al in de wet bij een dergelijk verzoek wordt voorgeschreven (artikel 29, tweede lid, en 50, tweede lid) ook de categorie van selectoren te benoemen; in de praktijk gebeurt dit al en via een beleidsregel kan dit ook worden vastgelegd.

Waar het gaat om punt 2a biedt artikel 39 van de wet (informantenregeling) al de mogelijkheid om ook buitenlandse diensten om gegevens, zoals geïntercepteerd materiaal, te vragen. Niettemin is het wenselijk om – als pendant van de expliciet geregelde mogelijkheid tot verstrekking van gegevens aan

buitenlandse diensten – ook de bevraging wettelijk te regelen; immers de vraag is of deze vorm van bevraging wel voldoende kenbaar en voorzienbaar is voor de burger. Voorlopig kan dit via een openbare beleidsregel worden geadresseerd (valt binnen het begrip “law” uit het EVRM). Het tweede element (punt 2b) betreft de toe te passen waarborgen op geïntercepteerd materiaal dat is verkregen van een buitenlandse dienst die geen partij bij het EVRM is. Deze dienen dezelfde te zijn als die welke het EHRM heeft gesteld in het kader van de interceptie door Staten die partij zijn bij het EVRM. Dit zal ook in de wet worden vastgelegd. Praktisch gezien betekent dit dat de regeling inzake verdere verwerking van dergelijke data uit de Wiv 2017 ook op de van buitenlandse diensten ontvangen gegevens dient te worden toegepast. Daartoe is uiteindelijk een wetswijziging vereist. Daarop vooruitlopend kan echter via een beleidsregel al in de vereiste waarborgen worden voorzien. Waar het gaat om de voorgeschreven TIB-toets op de door een minister verleende toestemming voor selectie en metadata-analyse van gegevens verkregen via eigen OOG-interceptie zal in overleg met de TIB dienen te worden bezien of een dergelijke toets waar het gaat om materiaal verkregen van een buitenlandse dienst voorlopig via een bindend advies-constructie kan worden vormgegeven.

Ten aanzien van punt 3 zal de bestaande regeling waar het gaat om de bescherming van journalistieke bronnen op een beperkt aantal onderdelen dienen te worden aangevuld. In verzoeken om selectie met het doel om gegevens te verkrijgen omtrent een bron van een journalist zullen de te hanteren selectoren en zoekvragen moeten worden opgenomen; dat kan in afwachting van aanpassing van de wet in een beleidsregel worden vastgelegd. Waar het gaat om de situatie dat bij de verwerking van geïntercepteerd materiaal – als bijvangst – op journalistiek materiaal wordt gestuit, zal de wet in een autorisatieprocedure moeten gaan voorzien voor voortdurende opslag en onderzoek. Het ligt voor de hand om dit ook bij de rechtbank Den Haag te beleggen. Voor de periode daaraan voorafgaand zal nader bezien moeten worden hoe deze autorisatie vorm te geven.

Deze aanpassingen – die deels ook door de Evaluatiecommissie Wiv 2017 zijn voorgesteld – kunnen bij de voorgenomen wijziging van de Wiv 2017 naar aanleiding van de evaluatie van de Wiv 2017 worden meegenomen.

Op het vlak van toetsing en toezicht bieden de uitspraken geen nieuwe inzichten, behalve dan dat – zie de Zweedse zaak – het onderbrengen van toezicht en klachtbehandeling (‘ex post facto review’) bij eenzelfde instantie voor het EHRM niet aanvaardbaar is indien dit leidt tot een situatie waarbij “de slager zijn eigen vlees keurt”. Vooralsnog moet ervan worden uitgegaan dat de in de Wiv 2017 neergelegde constructie waarbij de afdeling toezicht en de afdeling klachtbehandeling in één organisatie zijn ondergebracht - maar met een “Chinese muur” - de toets van het EHRM kan doorstaan. Het verdient evenwel aanbeveling om naar aanleiding van de Zweedse zaak te bezien of deze “Chinese muur” versterkt zou moeten worden.

Ook geven beide uitspraken geen aanleiding om anderszins te komen tot aanpassing van het bestaande toezichtsregime. Afgezien van bindende *autorisatie* vooraf, zoals in Nederland voorzien via de TIB (het EHRM noemt dit *autorisatie* in plaats van toezicht) en de bindende *klachtbehandeling* achteraf zoals voorzien via de afdeling klachtbehandeling van de CTIVD, wordt bindend toezicht door het EHRM niet als eis geformuleerd. Het EHRM oordeelde in de zaak Big Brother Watch tegen het VK inzake het toezicht door de *IC commissioner* nog expliciet op dat deze *“independent and effective supervision”* uitoefent. De *IC commissioner* beschikt niet over de bevoegdheid bindende oordelen te geven maar kan wel aanbevelingen doen, vergelijkbaar met de afdeling toezicht van de CTIVD.

In het kader van de evaluatie van de Wiv 2017 heeft de Evaluatiecommissie Wiv 2017 (verder: ECW) in januari 2021 een rapport uitgebracht, waarin – op basis van analyse van de door haar onderzochte vraagstukken en de daaruit getrokken conclusies – een 57-tal aanbevelingen gedaan. Het kabinet heeft in zijn reactie op dit rapport aangegeven de analyse, conclusies en aanbevelingen van de

commissie te omarmen, zij het dat er wel nadrukkelijk naar de uitvoeringsconsequenties zal worden gekeken. Later heeft het kabinet het parlement – aanvullend op de eerdere reactie – medegedeeld eerst met een hoofdlijnennotitie te komen (najaar 2021) en na bespreking met de Kamer pas aan de voorbereiding van het wetsvoorstel te beginnen. Een aantal aanbevelingen van de ECW voorziet al in regeling van aspecten waartoe ook de twee uitspraken van het EHRM aanleiding geven. Denk daarbij in het bijzonder aan aanbeveling 29 (grondslag bevraging internationale partners), 31 (inrichting en effectiviteit van het toezicht als afzonderlijk wegingscriterium), 32 (specifieke voorwaarden bij verstrekking van gegevens aan buitenlandse diensten), 34 (uniform verwerkingsregime voor bulkdata ook van toepassing op ontvangen bulkdata van buitenlande diensten; in casu hetzelfde principe maar dan voor geïntercepteerd materiaal). Een enkele aanbeveling van de ECW zal echter geen uitvoering kunnen krijgen, namelijk 8, waarbij men adviseert het toestemmingsniveau voor selectie intern bij de diensten te beleggen; de uitspraken van het EHRM staan hieraan in de weg.

Conventie 108+

Onder auspiciën van de Raad van Europa is op 28 januari 1981 te Straatsburg het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens tot stand gekomen (Trb. 1988, 7). Dit verdrag vormt een uitwerking van het door artikel 8 van het EVRM beschermde recht op eerbiediging van de persoonlijke levenssfeer met betrekking tot de geautomatiseerde verwerking van persoonsgegevens. Op 10 oktober 2018 is het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens tot stand gekomen (Trb. 2018, 201). Dit wijzigingsprotocol voorziet in een groot aantal inhoudelijke en institutionele wijzigingen die dermate substantieel zijn dat er materieel gezien een vrijwel geheel nieuw verdrag zal ontstaan (ook wel aangeduid als C-108+). De inhoudelijke wijzigingen brengen het niveau van gegevensbescherming binnen de Raad van Europa in lijn met het beschermingsniveau dat wordt geboden door het recht van de EU op dit gebied. Dit komt neer op het beschermingsniveau vergelijkbaar met de Algemene Verordening Gegevensbescherming (AVG).

De bestaande wet- en regelgeving (in het Europese deel van Nederland) is volledig in lijn met het gewijzigde verdrag. De Wiv 2017 bevat op enkele onderdelen afwijkende bepalingen, maar deze passen binnen het stelsel van uitzonderingen en beperkingen zoals toegestaan op grond van artikel 11 (nieuw) van het gewijzigde verdrag. Aan de CTIVD komt bijvoorbeeld niet de bevoegdheid tot interventie of het nemen van besluiten toe. Deze uitzondering/beperking is toegestaan (op grond van artikel 11, derde lid) waarbij geen afbreuk wordt gedaan aan onafhankelijk en effectief toezicht door de CTIVD, hetgeen ook blijkt uit het eerder aangehaalde oordeel van het EHRM over de Britse IC Commissioner in de zaak Big Brother Watch tegen het VK.

Stelsel van toezicht en democratisch-rechtsstatelijke checks and balances

Wat in Nederland wordt aangeduid als het ‘stelsel van toezicht op de inlichtingen- en veiligheidsdiensten’ omvat in ieder geval:

a. de autorisatie vooraf;
b. het ‘eigenlijke’, doorlopende en/of dynamische, toezicht en
c. de klachtbehandeling achteraf.

De EHRM-jurisprudentie stelt vooral eisen aan a en c. Binnen de bandbreedte van die eisen kan worden geconcludeerd dat de inrichting van het stelsel van toezicht (beleids)keuzes laat aan de wetgever. Deze bandbreedtes zijn dus het breedst ten aanzien van het doorlopende en/of dynamische toezicht, zoals in Nederland uitgeoefend door de afdeling toezicht van de CITVD (hierboven onder b).

Bij het maken van die keuzes is het van belang mee te wegen dat het voornamelijk op de leest van *rechtsstatelijkheid* geschoeide toezichtstelsel ook moet worden bezien in de bredere context van de *democratische* rechtsstaat. Democratische controle op de inlichtingen- en veiligheidsdiensten kent inherente uitdagingen. Veel van wat inlichtingen- en veiligheidsdiensten doen, kan niet in grote mate van detail in de openbaarheid worden gedeeld. Dat neemt het belang van democratische norm- en kaderstelling vooraf en democratische controle achteraf echter niet weg.

Vanuit een *rechtsstatelijk* perspectief kan worden aangegeven welke grenzen diensten in acht moeten nemen en kan tot op zekere hoogte worden aangeven welke ontwikkelingen in het takenpakket van diensten in meer of mindere mate passen in het rechtsstatelijke bestel. Niettemin, het antwoord op de fundamentele vraag wat de taken, prioriteiten, en (beleids)keuzes in het inlichtingen- en veiligheidswerk moeten zijn, kan alleen zijn gegrondvest in een *democratische* legitimatie en controle. De sleutel voor *democratische* controle ligt in de erkenning van het belang van ministeriële verantwoordelijkheid. De Nederlandse inlichtingen- en veiligheidsdiensten opereren onder volledige ministeriële verantwoordelijkheid. Hierachter schuilt dat ten aanzien van deze diensten (en hun verstrekkende bevoegdheden) moet worden vastgehouden aan volwaardig burgerlijk (politiek) gezag. Bij volledige ministeriële verantwoordelijkheid en volledig ministerieel gezag past maximale ministeriële zeggenschap. Het introduceren van nieuwe vormen van bindend toezicht op de diensten gaat ten koste van die zeggenschap. In de meest verstrekkende vorm zou bijvoorbeeld de keuze om de ruime en inhoudelijk vrijwel ongeclausuleerde bevoegdheid van de CTIVD om *aanbevelingen* te doen te wijzigen in een bevoegdheid om juridisch bindende *aanwijzingen* te geven ten koste gaan van de zeggenschap van de minister en via de ministeriële verantwoordelijkheid jegens de Kamers dus ook ten koste van de democratische controle op de diensten. De mogelijke introductie van rechterlijk toezicht op zulke aanwijzingen, neemt dat effect niet weg. Ook de rechter is niet democratisch gelegitimeerd en beschikt – net zomin als de CTIVD – over de begrotingsbevoegdheid om mogelijke financiële gevolgen van bindende aanwijzingen op te vangen.

Daarmee is niet gezegd dat de introductie van meer specifieke, nadere – al dan niet bindende – toezichtselementen juridisch uitgesloten zou zijn. Hier ligt een keuze voor de wetgever. Wel moet daarbij worden bezien welke conceptuele dilemma's daarbij voorliggen. Het concept van het *markttoezicht* kan hierbij niet onverkort leidend zijn. Dit houdt verband met het gegeven dat de ondertoezichtgestelden (de diensten) volledig tot de overheid moeten worden gerekend en bovendien uitsluitend belast zijn met exclusieve overheidstaken. Dit maakt het reguliere *handhavings*instrumentarium van het markttoezicht (last onder dwangsom/bestuursdwang, bestuurlijke boetes, 'naming and shaming') nauwelijks aangewezen. Ten aanzien van de *onderzoeksbevoegdheden* (de inzet van bevoegdheden voorafgaand aan de genoemde handhavingsbesluiten, zoals de plicht om mee te werken aan onderzoeken en informatie te verstrekken aan de toezichthouders) kan in de Wiv 2017 wel aansluiting worden gezocht. Voor een groot deel is dat al het geval.

Delen van het handhavingsinstrumentarium van het *interbestuurlijk toezicht* (schorsing, vernietiging, goedkeuring, aanwijzing, indeplaatsstelling) zouden in dat verband eerder aangewezen zijn, zij het dat het ook hier opvalt dat de (grond)wetgever er bij de toekenning van dergelijke bevoegdheden stelselmatig voor kiest deze te beleggen bij organen die zelf beschikken over een (al dan niet indirecte) democratische legitimatie. Deze legitimatie bestaat in de huidige praktijk op zijn minst uit een politiek te sanctioneren verantwoordingsrelatie. Alleen in acute crisissituaties, zoals voorzien in de Wet veiligheidsregio's bestaan hierop (tijdelijke) uitzonderingen. Het is aan de wetgever om te wegen of er in het toezicht op de inlichtingen- en veiligheidsdiensten reden is om van deze praktijk af te wijken.

Het uitgangspunt van democratische verantwoording zou dan wel vergen dat zwaarwegende (al dan niet bindende) oordelen in deze fase van het toezicht – door een orgaan dat zelf geen democratisch

verantwoordingmechanisme kent - helder moeten worden omlijnd. Dit zou dan in ieder geval opgaan voor wat betreft het toepassingsbereik, het soort bevoegdheid en de voor de ondertoezichtgestelde te gelden waarborgen in te volgen procedures.

Een andere conceptuele vraag is in hoeverre het toekennen van nieuwe, bindende, toezichtsinstrumenten (bijvoorbeeld in specifieke gevallen) gevolgen moet hebben voor de algemene en vrijwel ongeclausuleerde aanbevelingsbevoegdheid. Zonder daarbij te suggereren dat de vergelijking één-op-één opgaat, is bijvoorbeeld bij de Raad van State (op grond van Europese jurisprudentie) gekozen voor “Chinese muren” tussen de afdeling die bindende oordelen velt in specifieke gevallen en de afdeling die in brede zin adviseert.

Samenvattend is het vrijwel onvermijdelijk dat het toezicht op de inlichtingen- en veiligheidsdiensten een ‘sui generis’ karakter draagt en ook in de toekomst zal dragen. Ministeriële verantwoordelijkheid blijft daarbinnen de belangrijkste sleutel tot democratische controle. Daarbij bestaat uiteraard afwegingsruimte voor de wetgever, zij het dat deze niet onbegrensd is. Ter inspiratie kan altijd worden geput uit andere modellen van toezicht. Helder is wel dat geen enkel bestaand toezichtsmodel ‘als gegoten’ zit.

BIJLAGE - Puntsgewijze analyse recente uitspraken van het Europees Hof voor de Rechten van de Mens (EHRM) van 25 mei 2021 op de gevolgen voor de Wiv 2017

Algemeen inleidend

1. Op 25 mei 2021 heeft de Grote Kamer van het EHRM (hierna: het Hof – ter onderscheiding van de Kamer) een tweetal uitspraken gedaan, te weten in de zaken Big Brother Watch and others v. The United Kingdom (application nos. 58170/13, 62322/14 en 24960/15) en Centrum för Rättvisa v. Sweden (application no. 35252/08). In beide zaken gaat het om bulkinterceptie van telecommunicatie door inlichtingen- en veiligheidsdiensten en de verdere verwerking van de aldus verkregen gegevens. Daarbij speelt in de Britse zaak ook het vraagstuk van het ontvangen van bulkinterceptiegegevens van buitenlandse diensten en in de Zweedse zaak juist de verstrekking ervan aan buitenlandse diensten. Het belang van beide zaken ligt daarin dat het Hof komt tot aanpassing van zijn jurisprudentie aan de praktijk van bulkinterceptie van communicatie (en verkeersgegevens) en daarvoor een toetsingskader ontwikkelt. Het zijn in dat opzicht als zogeheten landmark-arresten te beschouwen. Op het nieuwe toetsings-/eisenkader zal in het onderstaande uitvoerig worden ingegaan. Ook zal worden ingegaan op de uitspraken van het Hof met betrekking tot artikel 10 EVRM en bulkinterceptie. Niet zal worden ingegaan op de beschouwingen inzake de ontvankelijkheid van de klagers in genoemde zaken. Dat geldt ook voor de bij de uitspraken gevoegde Concurring en Dissenting Opinions; immers juridisch relevant zijn uitsluitend de door de Grote Kamer gedane uitspraken.
2. In het onderstaande wordt – waar dat aan de orde is - ingegaan op de gevolgen die deze uitspraken (mogelijkerwijs) kunnen hebben voor de Wiv 2017. Waar het gaat om de uitwerking van de aanbevelingen van de Evaluatiecommissie Wiv 2017 (ECW) alsmede de mogelijke gevolgen van het nieuwe dataprotectieverdrag van de Raad van Europa (aangeduid als C-108+), zoals dat komt te luiden als gevolg van het – nog door Nederland te ratificeren - Protocol tot wijziging van C-108, wordt in de oplegnota bij deze analyse nog in het kort ingegaan.
3. Tot slot is het goed om het volgende in algemene zin op te merken. Zoals in alle zaken van het EHRM beoordeelt het Hof het aan hem voorgelegde feitencomplex en het wettelijk kader waarbinnen door de (instanties van de) Staten is geopereerd in het licht van het EVRM en de jurisprudentie van het EHRM. Het gaat daarbij om een holistische benadering; zo wordt bijvoorbeeld gekeken naar het hele stelsel van waarborgen dat geldt, de (onafhankelijke) positie van de instanties belast met toetsing en toezicht, waarbij de afwezigheid van de ene waarborg (bijvoorbeeld notificatie) kan worden gecompenseerd door de aanwezigheid van een ander waarborg (bijvoorbeeld de aanwezigheid van een ruime klachtmogelijkheid) enz. Dat betekent dat enige voorzichtigheid is geboden bij het doortrekken van de door het EHRM getrokken conclusies in een aan hem voorgelegde zaak naar het eigen rechtstelsel. Of uiteindelijk het eigen rechtstelsel aan het EVRM voldoet is immers – vaste jurisprudentie – ter finale beoordeling van het EHRM. Wel zijn er door het EHRM in de loop van de jaren in de vorm van vaste jurisprudentie diverse eisen geformuleerd die worden gehanteerd bij de beoordeling van voorgelegde zaken; zo spelen in de onderhavige twee zaken de zgn. Weber-criteria een rol, die thans – toegespitst op de bevoegdheid tot bulkinterceptie – nader worden uitgewerkt.

Big Brother Watch e.a. tegen het Verenigd Koninkrijk

A. Bulkinterceptie

1. In deze zaak gaat het primair om bulkinterceptie door de Britse dienst van zogeheten grensoverschrijdende ("cross border") communicatie; dat wil zeggen communicatie met oorsprong of bestemming in het buitenland. Bulkinterceptie van (louter) binnenlands verkeer is in het VK niet geoorloofd (mocht men op dergelijke informatie stuiten dan dient dat vernietigd te worden) en staat dan ook niet ter beoordeling.

   De Wiv 2017 kent een dergelijke beperking niet. Ten opzichte van het Britse (maar ook Zweedse) stelsel is de geografische reikwijdte van het Nederlandse bulkinterceptiestelsel derhalve ruimer.

2. Het Hof stelt vast dat – gaande de procedure – is vast te komen staan dat het beoordelen van dit soort bulkinterceptieregimes specifieke moeilijkheden met zich mee brengt. Bij bulkinterceptie spelen andere problematieken dan bij gerichte interceptie. Voorts constateert het Hof dat de ontwikkelde jurisprudentie primair betrekking heeft op het opsporingsveld, terwijl bulkinterceptie veeleer op het vlak van vergaring van buitenlandse inlichtingen en de onderkenning van dreiging van bekende en onbekende actoren wordt gebruikt. Daar speelt natuurlijk ook mee dat waar het gaat om het nationale veiligheidsdomein waarin dergelijke bevoegdheden worden ingezet de Staten om legitieme redenen geheimhouding betrachten en er dus in het publieke domein weinig bekend zal zijn. Het Hof stelt dan ook uiteindelijk: *"Consequently, the Court is required to carry out its assessment of Contracting States' bulk interception regimes, a valuable technological capacity to identify new threats in the digital domain, for Convention compliance by reference to the existence of safeguards against arbitrariness and abuse, om the basis of limited information about the manner in which those regimes operate."* (ov 323).

3. Het Hof ziet bulkinterceptie als een gradueel proces waarbij de mate van inmenging met de in artikel 8 EVRM vastgelegde rechten van een persoon toeneemt naargelang het proces zich verder ontwikkelt. (ov 325). Hoewel het Hof erkent dat niet ieder bulkinterceptie-regime hetzelfde is en volgens dezelfde chronologie hoeft te verlopen ziet het Hof de volgende vier stadia, die vervolgens nader worden bezien:
   i. De interceptie en initiële bewaring van communicatie (inhoud) en de gerelateerde communicatiedata (verkeersgegevens);
   ii. De toepassing van specifieke selectoren op de bewaarde communicatie/communicatiedata;
   iii. Het onderzoek van geselecteerde communicatie/communicatiedata door analisten;
   iv. De daaropvolgende bewaring van gegevens en het gebruik van het "eindproduct", met inbegrip van het delen van data met derde partijen.

   In de Wiv 2017 kennen we in het kader van interceptie de handeling die bekend staat als "search gericht op interceptie" en in het kader van selectie de handeling die bekend staat als "search gericht op selectie" (artikel 49, eerste resp. tweede lid). De vraag is in welke door het Hof geformuleerde stadia deze twee handelingen zijn te positioneren.

   Het Hof acht artikel 8 EVRM van toepassing op al deze fasen, waarbij het Hof opmerkt dat de mate van inmenging toe zal nemen naar gelang het bulkinterceptieproces verder vordert. Ook het enkele bewaren van gegevens levert al een inmenging met artikel 8 op en de noodzaak voor waarborgen voor de bescherming van persoonsgegevens zal groter zijn

indien de gegevens worden onderworpen aan geautomatiseerde verwerking. Aan het slot – waar de inhoud van de communicatie van een persoon wordt onderzocht door een analist – zal de noodzaak voor waarborgen het grootst zijn. (ov. 325-331)

4. Het Hof gaat vervolgens in op de algemene principes die hij hanteert waar het gaat om geheime surveillance-maatregelen, waaronder begrepen de interceptie van communicatie. Relevante noties uit het betoog van het Hof zijn de volgende:

   - *"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* (artikel 8 lid 2) *has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements. The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse."* (ov. 334).

   - Tegen deze achtergrond en toegespitst op interceptie in strafrechtelijke onderzoeken (criminal investigations) heeft het hof de zogeheten Weber-criteria ontwikkeld, die in wetgeving ("law") moeten zijn neergelegd. Deze criteria betreffen:
     i. the nature of the offences which may give rise to an interception order;
     ii. a definition of the categories of people liable to have their communications intercepted;
     iii. a limit on the duration of interception;
     iv. the procedure to be followed for examining, using and storing the data obtained;
     v. the precautions to be taken when communicating the data to other parties; and
     vi. the circumstances in which intercepted data may or must erased or destroyed.

     Deze criteria zijn vervolgens door het Hof ook toegepast in zaken waar de interceptie plaatsvond in het kader van nationale veiligheid (zaak Roman Zakharov); maar – zoals het Hof aangeeft – bij het vaststellen of de betreffende wetgeving in strijd was met artikel 8 EVRM moest het ook acht slaan op de maatregelen (*arrangements*) voor de supervisie op de toepassing van de geheime surveillance-maatregelen, de aanwezigheid van notificatie-mechanismen en de remedies die door het nationale recht worden geboden (ov. 335).

     De genoemde Weber-criteria (of Zakharov-criteria) zijn bij het ontwerpen van de Wiv 2017 nadrukkelijk tot uitgangspunt genomen; in hoofdstuk 9 van de memorie van toelichting bij het wetsvoorstel is ingegaan op de wijze waarop deze criteria in de wet uitwerking hebben gekregen.
   - Teruggrijpend op het Klass-arrest uit 1978 wijst het Hof op de drie fasen van onderzoek waarbij review en supervisie van geheime surveillance-maatregelen aan de orde is: wanneer surveillance wordt bevolen, wordt uitgevoerd en nadat het is beëindigd. Bij de eerste twee fasen brengt de aard en logica van geheime surveillance met zich mee dat niet alleen de uitvoering maar ook het toezicht daarop (*accompanying review*) zonder kennis bij de betrokken persoon zal dienen plaats te vinden. Dit gegeven brengt met zich mee dat de gehanteerde procedures op zichzelf voorzien in *"adequate and equivalent guarantees"* ter bescherming van de rechten van betrokkene. In dat verband heeft het Hof – bij herhaling – aangegeven dat het in principe wenselijk is dat toezicht

("*supervisory control*") wordt toevertrouwd aan een rechter, aangezien die de beste garanties voor onafhankelijkheid, onpartijdigheid en een juiste procedure biedt. (ov. 336) Ook een niet rechterlijke-instantie is mogelijk, mits deze instantie op vergelijkbare wijze aan deze eisen voldoet.

- Met betrekking tot de derde fase kijkt het Hof met name naar de aanwezigheid van een notificatiemechanisme ertoe strekkende dat betrokken wordt geïnformeerd over het feit dat hij onderworpen is aan onderzoek en de rechtmatigheid daarvan kan laten onderzoeken dan wel – als alternatief – dat een ieder die vermoedt dat deze is onderworpen aan surveillance ter zake naar een rechter kan stappen (*apply the courts*), waarvan de rechtsmacht niet afhankelijk is van notificatie aan betrokkene. (ov. 337)

  In de Wiv 2017 wordt voorzien in notificatie in een aantal limitatieve gevallen (bulkinterceptie evenwel uitgezonderd), maar staat altijd de mogelijkheid open om of naar de rechter te stappen (veelal civielrechtelijke weg) of een bindend oordeel van de onafhankelijke afdeling klachtbehandeling bij de CTIVD te krijgen.

- Erkennende dat de Staten een ruime marge hebben om te bepalen op welke wijze zij de nationale veiligheid het beste kunnen beschermen, is die marge – aldus het Hof – wel onderworpen aan toezicht door het EHRM dat zowel de wetgeving als de (besluiten ter) uitvoering daarvan betreft. Hier komt dan de holistische benadering van het Hof (beoordeling van het stelsel als geheel in al zijn facetten) aan de orde. (ov. 338, 339)

5. Het Hof gaat vervolgens in op de vraag of het noodzakelijk is om de jurisprudentie (verder) te ontwikkelen en – na een bevestigend antwoord – presenteert het vervolgens de benadering die toegepast dient te worden op bulkinterceptie-zaken. (ov. 340 e.v.; resp. 348 e.v.)

6. Al eerder heeft het Hof erkend dat in het kader van het onderkennen van dreigingen tegen de nationale veiligheid de toepassing van bulkinterceptie – onder voorwaarden – is geoorloofd. De eerder genoemde zes Weber-criteria zijn echter ook al meer dan 10 jaar oud en de technologische ontwikkelingen alsmede de wijze waarop mensen communiceren hebben in de tussentijd niet stilgestaan. *"Lives are increasingly lived online, generating both a significantly larger volume of electronic communications, and communications of a significantly different nature and quality, to those likely to have been generated a decade ago."* (ov. 341) In dat verband wijst het Hof erop dat in vergelijking met nu, de reikwijdte van de surveillance-activiteit toentertijd beperkter was. Dat geldt niet alleen voor (de toename van) het volume aan communicatie (inhoud) maar evenzeer voor de aan de communicatie gerelateerde communicatiedata (verkeersgegevens). Daarbij komt dat verkeersgegevens veel persoonlijke informatie kunnen prijsgeven, zoals de identiteit en de geografische locatie van de zender en ontvanger en de gebruikte apparatuur waarmee communicatie wordt overgebracht. De daarmee gepaard gaande inbreuk wordt alleen maar groter ingeval sprake is van bulkverwerving met name door de thans voorhanden zijnde analysemethoden waardoor een intiem portret van personen kan worden verkregen. (ov. 342) Belangrijker is, aldus het Hof, dat men in bijvoorbeeld de Weber-zaak uit 2008 niet nadrukkelijk rekening heeft gehouden heeft met het feit dat het om een vorm van surveillance van een geheel andere aard en schaal ging dan in daaraan voorafgaande zaken aan de orde was. Gerichte interceptie en bulkinterceptie zijn immers in diverse opzichten verschillend:

i. Bulkinterceptie is veelal gericht op internationaal communicatieverkeer, waarbij het doel is om de communicaties te monitoren van personen buiten de eigen jurisdictie die niet door andere vormen van surveillance kunnen worden gemonitored. (ov. 344)

Dit argument – los van het feit dat in Nederland bij bulkinterceptie geen geografische beperking bestaat – geldt ook bij de inzet van bulkinterceptie door de Nederlandse diensten, nu de inzet van gerichtere bevoegdheden in het buitenland (buiten de eigen jurisdictie) veelal niet mogelijk is.

ii. Ook het doel waarvoor bulkinterceptie wordt uitgevoerd lijkt anders te zijn dan bij gerichte interceptie. De inzet van bulkinterceptie lijkt vooral gebruik te worden voor doeleinden van buitenlandse gegevensverzameling (*foreign intelligence gathering*), de vroege ontdekking en onderzoek van cyberaanvallen, contra-spionage en contra-terrorisme. (ov. 344)

iii. Bulkinterceptie wordt niet noodzakelijkerwijs gebruikt om op specifieke onderzoeksubjecten (targets) te worden toegepast, maar het kan wel en niet zozeer door het monitoren van hun apparatuur maar door het gebruik van "*strong selectors*" (zoals e-mailadressen) op de in bulk verzamelde gegevens. Of door toepassing van een "*complex query*". (ov. 346)

Afgezet tegen deze achtergrond stelt het Hof vast dat – zoals bij elk interceptieregime – er bij bulkinterceptie natuurlijk een aanzienlijke mogelijkheid bestaat dat deze op een manier wordt gebruikt die nadelig is voor het recht op privéleven van de burger. Hoewel artikel 8 EVRM de toepassing van bulkinterceptie in het kader van nationale veiligheid niet verbiedt, stelt het Hof wel dat bij de toepassing daarvan de "*margin of appreciation*" (die de Staten ter zake toekomt) beperkter moet zijn en tevens moet er een aantal waarborgen aanwezig zijn. Dit leidt tot vaststelling van een aangepast kader voor bulkinterceptie-zaken; daarbij wordt voortgebouwd op de eerder ontwikkelde Weber-criteria. (ov. 347)

7. Voorafgaand aan de presentatie van de nieuwe acht criteria die het Hof – als minimum voorwaarden – stelt aan een bulkinterceptie-regime, beziet het Hof of en, zo ja, in hoeverre de Weber-criteria bij bulkinterceptie toepassing kunnen vinden. Afgezien van de laatste vier criteria, die bij bulkinterceptie ook van toepassing zijn, overweegt het Hof met betrekking tot de eerste twee criteria (omschrijving van "*nature of the offences*" en "*categories of people*") dat die niet zonder meer van toepassing kunnen zijn en derhalve vervangen dienen te worden door andere criteria. (ov. 348)

8. Daarnaast besteedt het Hof uitvoerig aandacht aan de arrangementen voor toezicht en controle (*supervising and reviewing*) op het interceptieregime, waarvan het belang in de context van bulkinterceptie versterkt *(amplified)* is vanwege het inherente risico op misbruik en omdat de legitieme noodzaak tot geheimhouding onvermijdelijk betekent dat – voor redenen van nationale veiligheid – Staten vaak niet de vrijheid hebben om informatie openbaar te maken betreffende de werking van het betwiste regime. In dat kader overweegt het Hof het volgende: *"Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorization at the outset, when the*

object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review.*"* In de ogen van het Hof zijn dit de fundamentele waarborgen die de hoeksteen dienen te vormen van elk bulkinterceptie-regime om in overeenstemming met artikel 8 EVRM te kunnen zijn. (ov. 350)

9. Het Hof werkt een en ander met betrekking tot een aantal belangrijke aspecten nader uit:

   i. Waar het gaat om autorisatie geldt rechterlijke autorisatie als een belangrijke waarborg tegen willekeur, maar is niet een noodzakelijk vereiste; wel dient bulkinterceptie onderworpen te zijn aan autorisatie door een onafhankelijk lichaam, dat wil zeggen: onafhankelijk van de uitvoerende macht. (ov. 351)

      In het Nederlandse stelsel is de autorisatie feitelijk in twee delen geknipt, eerst toestemming van de minister en vervolgens goedkeuring van de toestemming van de minister door de TIB. Zonder de goedkeuring van de TIB vervalt de verleende toestemming van de minister van rechtswege. De autorisatie heeft derhalve bindend karakter.

   ii. Om een effectieve waarborg tegen misbruik te kunnen vormen dient het onafhankelijke autoriserende lichaam geïnformeerd te worden omtrent zowel het doel van interceptie als de dragers van communicatie-routes (*bearers of communication routes*) die waarschijnlijk worden geïntercepteerd. Daarmee kan niet alleen de noodzakelijkheid en proportionaliteit van de bulkinterceptie operatie worden getoetst maar ook kan aldus worden bepaald of de selectie van de dragers noodzakelijk en proportioneel is voor het doel waarvoor de interceptie wordt uitgevoerd. (ov. 352)

      De "dragers van de communicatie-routes" lijken te duiden op de specifieke kabels die worden geïntercepteerd. In de aanvraag voor een toestemming op grond van de Wiv 2017 dient vrij concreet te worden bepaald welk specifiek deel van de kabelinfrastructuur dient te worden geïntercepteerd en wat voor soort verkeer dient te worden geïntercepteerd. Dit dient te zijn getoetst aan de eisen van noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid (artikel 18 Wiv 2017). De TIB toetst de verleende toestemming vol op deze aspecten en kan – voor zover dat voor een goede taakuitvoering noodzakelijk is – alle relevante informatie ter zake ontvangen.

   iii. Het gebruik van selectoren – en "*strong selectors*" (zoals e-mailadressen) in het bijzonder – acht het Hof een van de belangrijkste stappen in het bulk interceptieproces, omdat dat het moment is waarop de diensten gericht de communicatie van een bepaalde persoon kunnen benaderen. Alles afwegende (onder meer naar aanleiding van de inbreng van Nederland en het VK) accepteert het Hof dat, rekening houdend met de karakteristieken van bulkinterceptie, het grote aantal selectoren dat wordt gebruikt en de inherente noodzaak voor flexibiliteit in de keuze van selectoren, het opnemen van alle selectoren in een (het verzoek om) autorisatie in de praktijk niet werkbaar is. Niettemin, gegeven het feit dat de keuze van de selectoren en de zoektermen (*query terms*) bepaalt welke communicatie in aanmerking komt voor onderzoek door een analist, dient de

autorisatie op zijn minst de typen of categorieën van selectoren die worden gebruikt te identificeren. (ov. 354)

In artikel 50, tweede lid, Wiv 2017 dient in het verzoek om toestemming voor selectie – in aanvulling op de algemene eisen van artikel 29 - de identiteit van de persoon of organisatie of een omschrijving van het onderwerp ten aanzien waarvan de bevoegdheid (tot selectie) wordt toegepast, te worden gegeven. De daartoe door de minister verleende toestemming wordt door de TIB getoetst (autorisatie). Onduidelijk blijft wat nu de precieze reikwijdte is van "type of categorieën van selectoren", dus ook of de geëiste autorisatie ook ziet op toe te passen categorieën *query terms* (zoekvragen/algoritmen) op de bulk aan communicatie.

iv. Waar het gaat om het gebruik door de diensten van "*strong selectors*" (zoals e-mailadressen) die gelinkt zijn aan identificeerbare (*identifiable*) personen dienen er versterkte waarborgen aanwezig te zijn. Het gebruik van iedere selector (*every such selector*) moet – gelet op de eisen van noodzakelijkheid en proportionaliteit – worden gerechtvaardigd en dat moet nauwkeurig worden vastgelegd en worden onderworpen aan een proces van voorafgaande interne autorisatie die voorziet in een afzonderlijke en objectieve verificatie waarbij wordt bezien of de rechtvaardiging voldoet aan de genoemde eisen. (ov. 355)

In artikel 50, derde lid, Wiv 2017 is bepaald dat de vaststelling van de concrete selectiecriteria plaatsvindt door de minister dan wel het hoofd van de dienst; ondermandaat is mogelijk. Ieder selectiecriterium dient van een toereikende motivering te worden voorzien in relatie tot het onderzoek waarvoor de worden toegepast.

v. Iedere fase van het bulkinterceptieproces – met inbegrip van de initiële autorisatie en daaropvolgende vernieuwingen (*renewals*), de selectie van de dragers, de keuze en toepassing van selectoren en zoektermen, en het gebruik, de opslag, de doorverstrekking en het wissen van geïntercepteerd materiaal – moet ook onderworpen zijn aan toezicht door een onafhankelijke autoriteit en dat toezicht dient voldoende robuust te zijn teneinde de inmenging (*interference*) binnen de grenzen van wat noodzakelijk is in een democratische samenleving te houden. In het bijzonder dient de toezichthouder in een positie te zijn om de noodzaak en proportionaliteit van de ondernomen actie(s) te beoordelen, waarbij men acht slaat op (*having due regard to*) het overeenkomstige niveau van inmenging in de rechten uit het verdrag met betrekking tot de persoon die het betreft. (ov. 356)

De afdeling toezicht van de CTIVD ziet toe op de rechtmatigheid van de uitvoering van de Wiv 2017 en daarmee ook op het gehele bulkinterceptieproces. In dat kader – zie ook de vele rapporten die sinds 2003 door de CTIVD zijn uitgebracht – toetst de CTIVD (waar sprake is van een inbreuk op bijvoorbeeld het recht ex artikel 8 EVRM) aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Daartoe kan zij over alle relevante informatie beschikken (onder meer rechtstreeks geautomatiseerde toegang tot de informatiesystemen bij de diensten). De toezichtsrapporten worden met een reactie van de minister openbaar en de minister kan ter zake door het parlement ter verantwoording worden

geroepen. Het Nederlandse stelsel van toezicht is daarmee effectief en robuust zoals bedoeld door het Hof.

vi. Tot slot dient er een "*effective remedy*" beschikbaar te zijn voor iedereen die vermoedt dat zijn of haar communicatie door de diensten is geïntercepteerd, waarbij de rechtmatigheid van de vermoede interceptie dan wel de verdragsconformiteit van het interceptieregime kan worden betwist. Ook hier geldt dat notificatie van de betrokkene niet als eis geldt indien het systeem van binnenlandse remedies een ieder toestaat om zich tot een rechter (*courts*) te wenden indien door hem of haar wordt vermoed dat zijn of haar communicatie is geïntercepteerd. Een remedie die niet afhankelijk is van notificatie acht het Hof dan ook een effectieve remedie en zal, afhankelijk van de omstandigheden, zelfs betere waarborgen voor een juiste procedure (kunnen) bieden dan een remedie gebaseerd op notificatie. (ov. 357)

De Wiv 2017 voorziet niet in notificatie waar het gaat om (selectie op) bulkinterceptie van communicatie. Wel kent de wet de mogelijkheid voor een ieder bij de afdeling klachtbehandeling van de CTIVD een klacht in te dienen over opreden of vermeende optreden van – kort gezegd – de diensten (artikel 114, eerste lid).

vii. Het Hof gaat vervolgens nog in op de bevoegdheden en procedurele garanties waarover een autoriteit moet beschikken teneinde te bepalen of de remedie effectief is (*whether a remedy is effective*). Ter zake stelt zij: *"Therefore, in the absence of a notification requirement it is imperative that the remedy should be before a body which, while not necessarily judicial, is independent of the executive and ensures the fairness of the proceedings, offering, in so far as possible, an adversarial process. The decisions of such authority shall be reasoned and legally binding with regard, inter alia, to the cessation of unlawful interception and the destruction of unlawfully obtained and/or stored intercept material."* (ov. 359)

De afdeling klachtbehandeling is onafhankelijk (ook ten opzichte van de afdeling toezicht van de CTIVD) en beoordeelt of in de door haar onderzochte aangelegenheid behoorlijk is gehandeld; dat is een breed criterium, dat ook rechtmatigheid omvat. Klager en beklaagde worden daarbij gehoord. Het oordeel van de afdeling klachtbehandeling dient te worden gemotiveerd, is bindend en wordt openbaar gemaakt, zij het dat informatie die de nationale veiligheid kan schaden achterwege dient te blijven.

10. In het licht van het voorgaande bepaalt het Hof of een bulkinterceptieregime verdragsconform is en wel door een globale beoordeling van de werking van het regime. Daarbij, in het bijzonder of de Staat binnen zijn toekomende "marge van appreciatie" (*margin of appreciation*) is gebleven en meer specifiek, teneinde vast te stellen of wordt voldaan aan de eisen van "in overeenstemming met de wet" en "noodzakelijkheid" onderzoekt het Hof of in het binnenlands wettelijk kader de volgende acht eisen helder zijn bepaald (ov. 361):
    i. The grounds on which bulk interception may be authorized;
    ii. The circumstances in which an individual's communications may be intercepted;
    iii. The procedure to be followed for granting authorisation;

iv. *The procedures to be followed for selecting, examining and using intercept material;*
v. *The precautions to be taken when communicating the material to other parties;*
vi. *The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;*
vii. *The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;*
viii. *The procedures for independent ex post facto review of such compliance and the powers vested in the competent body addressing instances of non-compliance.*

11. Ter afsluiting van het betoog over toe te passen toetsingskader bij bulkinterceptie, gaat het Hof ook nog in op (1) de verstrekking van gegevens uit bulkinterceptie aan andere partijen, in het bijzonder aan buitenlandse Staten en internationale organisaties en (2) het onderscheid tussen bulkinterceptie van inhoud van communicatie en gerelateerde communicatiedata.(ov. 362-364)

12. Waar het gaat om internationale uitwisseling van gegevens uit bulkinterceptie stelt het Hof het volgende eisenkader op. De verstrekking (*transmission*) van gegevens verworven door bulkinterceptie moet worden beperkt tot gegevens die zijn verzameld en opgeslagen op een wijze die in overeenstemming is met het verdrag en moet onderworpen zijn aan enkele – vier - additionele waarborgen waar het gaat om de verstrekking als zodanig (*pertaining to the transfer itself*):
    i. De omstandigheden waaronder een dergelijke verstrekking plaats mag vinden moet helder uiteengezet zijn in nationaal recht;
    ii. De verstrekkende Staat moet verzekeren (*must ensure*) dat de ontvangende Staat, waar het gaat om de verwerking (*handling*) van gegevens, heeft voorzien in waarborgen waarmee misbruik en disproportionele inmenging (met het recht op privacy) wordt voorkomen. In het bijzonder moet die Staat de veilige opslag van de gegevens waarborgen en de verdere verstrekking (*onward disclosure*) beperken. Dit laatste betekent niet dat men over vergelijkbare bescherming als de verstrekkende Staat moet beschikken noch dat voorafgaand aan iedere verstrekking verzekering van de aanwezigheid van die waarborgen is gegeven.
    iii. Extra waarborgen zijn vereist indien helder is dat er gegevens worden verstrekt die bijzondere vertrouwelijkheid vereisen, zoals vertrouwelijke journalistieke gegevens.
    iv. De verstrekking van gegevens aan buitenlandse inlichtingenpartners moet onderworpen zijn aan onafhankelijk toezicht (*independent control*). (ov. 362)

13. Waar het gaat om het onderscheid tussen verkeersgegevens en inhoud van communicatie stelt het Hof niet overtuigd te zijn dat de verwerving van gerelateerde communicatiedata (verkeersgegevens) door bulkinterceptie minder inbreukmakend is dan de verwerving van inhoud. Om die reden dient de verwerving, het bewaren en het doorzoeken van gerelateerde verkeersgegevens (*related communications data)* door het Hof aan dezelfde waarborgen te worden getoetst als die welke gelden voor de inhoud van communicatie (ov. 363). In aanvulling – en ook ter relativering daarvan – stelt het Hof nog het volgende: *"That being said, while the interception of related communications data will normally be authorised at the same time the interception of content is authorised, once obtained they may be treated differently by the intelligence services (…). In view of the different character of related communications data and the different ways in which they are used by the intelligences services, as long as the aforementioned safeguards are in place, the Court is of*

the opinion that the legal provisions governing the treatment may not necessarily have to be identical in every respect to those governing the treatment of content." (ov. 364)

14. Tegen de hiervoor geschetste achtergrond (het voor bulkinterceptie en verdere verwerking ontwikkelde normenkader) onderzoekt het Hof vervolgens de voorgelegde zaak. Nu dit een beoordeling van het Britse stelsel (als geheel) is en de oordelen van het Hof daarover contextgebonden zijn, zullen uit de overwegingen van het Hof ter zake slechts die elementen in het onderstaande worden benoemd die in algemene zin van belang (kunnen) zijn bij de beoordeling van de door het Hof gestelde eisen in relatie tot het Nederlandse stelsel. Daarbij zal de wijze waarop het Nederlandse stelsel aan de door het Hof geformuleerde eisen en de inkleuring daarvan in het licht van het Britse stelsel zoals hieronder weergegeven, worden uiteengezet. Het Hof beziet daarbij allereerst de nieuwe geformuleerde eisen in relatie tot de inhoud van communicatie:

    i. Een (wettelijk) regime dat bulkinterceptie toelaat op relatief brede gronden (*wide grounds*) kan nog steeds in overeenstemming zijn met artikel 8 EVRM mits – als geheel bezien – er voldoende waarborgen tegen misbruik in het systeem zijn ingebouwd die deze zwakte compenseert. (ov. 370). [betreft eerste eis]

        In de Wiv 2017 is de uitoefening van de bijzondere bevoegdheid tot onderzoeksopdrachtgerichte (OOG) interceptie alleen mogelijk voor zover dat noodzakelijk is voor een goede taakuitvoering van de dienst. Die goede taakuitvoering is gerelateerd aan de taken die in artikel 8, tweede lid, onder a en d, en 10, tweede lid, onder a, c en e, aan AIVD onderscheidenlijk MIVD zijn toebedeeld en uitwerking hebben gekregen in de Geïntegreerde Aanwijzing. Daarbij is het overkoepelende belang de nationale veiligheid.

    ii. Bij de tweede eis is met name de keuze van de dragers en de beperking tot die dragers waarop communicatie die hoogstwaarschijnlijk van belang is vanuit nationale veiligheidsbelang (mede) bepalend. Die keuze bepaalt (mede) de kring van personen waarop de interceptie betrekking heeft, waarbij ook het feit dat verzender noch ontvanger controle hebben op de routering van het (IP) verkeer medebepalend zijn. (ov. 376)

        In de Wiv 2017 dient het verzoek om bulkinterceptie niet alleen te voldoen aan de algemene eisen van artikel 29, tweede lid, en de aanvullende eisen van artikel 48, derde lid. In het verzoek moet naast specificering van het doel, in het bijzonder de onderzoeksvragen die beantwoord moeten worden, ook de noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid van de voorgenomen bulkinterceptie worden beargumenteerd. Dit geheel kadert de toepassing van de bevoegdheid in en bepaalt onder welke condities deze kan worden ingezet.

    iii. Bij de derde eis lijkt het Hof niet de harde eis te stellen dat in de autorisatie voor bulkinterceptie (de warrant) precies is aangegeven welke dragers worden geïntercepteerd (*specify particular bearers*), maar dat volstaan kan worden met een adequate omschrijving van waarop de interceptie betrekking heeft en gedetailleerde informatie over de soort dragers die worden geïntercepteerd. (ov. 380) Wel wordt het ontbreken van iedere vorm van toezicht op de categorie van selectoren het VK aangerekend; aandachtspunt is (naast voorafgaande onafhankelijke autorisatie van

de categorie van selectoren) – bij het gebruik van "*strong selectors*" gelinkt aan identificeerbare personen – de noodzaak van een voorafgaande interne autorisatie daarvan. (ov. 383)

Zie allereerst opmerking onder ii. In aanvulling daarop wordt nog het volgende geconcludeerd. In artikel 50 Wiv 2017 is erin voorzien dat de minister moet instemmen met selectie, waarbij in het verzoek om toestemming – in aanvulling op het bepaalde in artikel 29, tweede lid – de identiteit van de persoon of organisatie of een omschrijving van het onderwerp ten aanzien waarvan de selectie-bevoegdheid moet worden toegepast wordt gegeven. Een verleende toestemming is vervolgens onderworpen aan de TIB-toets. De wettelijk voorgeschreven inhoud van een verzoek om toestemming komt niet overeen met hetgeen het Hof eist. De wet zal hiermee in overeenstemming moeten worden gebracht, zij het dat in de praktijk al wel EHRM-conform wordt gewerkt. Wel is het aangewezen dit in beleidsregels vast te leggen.

iv. Bij de vierde eis is van belang dat de toegang tot de geïntercepteerde gegevens zodanig is vormgegeven dat daarmee de omvang van de inbreuk op privacy (sterk) wordt beperkt; dat geschiedt door beperking van de kring van de personen die toegang hebben (autorisaties) maar ook door het specificeren van de gegevens waartoe die personen dan toegang hebben. Een en ander moet voldoen aan de eis van voorzienbaarheid. (ov. 386-391)

Op grond van de Wiv 2017 geldt in algemene zin het need-to-know-beginsel. Daarnaast rust op het hoofd van de dienst onder meer de plicht om de personen aan te wijzen die bij uitsluiting van anderen bevoegd zijn tot de bij de aanwijzing vermelde werkzaamheden in het kader van de verwerking van gegevens (artikel 24, tweede lid). Zowel in het kader van de bulkinterceptie van communicatie als de verdere verwerking daarvan (artikel 48, 49 en 50) worden voor specifiek werkzaamheden – waaronder het kennis mogen nemen van de inhoud van de geïntercepteerde communicatie - personen aangewezen die bij uitsluiting van anderen bepaalde werkzaamheden mogen verrichten. Het betreft hier een stelsel van functiescheiding.

v. Bij de vijfde eis wordt ook gekeken naar de regeling voor interne verstrekking (eisen die daaraan gesteld worden, zoals *need to know*), maar – in de voorliggende casus – met name naar de doorgifte van geïntercepteerde gegevens naar buitenlandse diensten of internationale partners (*outside the UK*); de externe verstrekking. Zie hetgeen hierboven onder 12 is gesteld. Het lijkt erop bij de interpretatie van "*to ensure*" (verzekeren) dat er bij de desbetreffende partner allerhande waarborgen voorhanden zijn, dit niet zo strikt (als letterlijke lezing van het begrip lijkt te veronderstellen) wordt genomen, nu in het VK dit blijkens de IC Code gaat om "*reasonable steps*" die door de verstrekkende dienst genomen moeten worden om te verzekeren dat de ontvangende autoriteiten de noodzakelijke procedures en waarborgen onderhouden. Dat wordt – naast andere waarborgen (zoals derde land-regel) – door het Hof blijkbaar voldoende geacht. Wel wordt nogmaals erop gewezen dat het Hof bijzonder gewicht toekent aan het toezicht dat door de IC commisioner en de IPT wordt uitgeoefend op een en ander. (ov. 396)

De diensten werken alleen samen met buitenlandse diensten waarvoor op grond van artikel 88 Wiv 2017 aan de hand van een wegingsnotitie is vastgesteld of met de betreffende dienst kan worden samengewerkt en, zo ja, wat de aard en intensiteit daarvan is. In die weging wordt onder meer bezien de eerbiediging van mensenrechten door het desbetreffende land en het door de desbetreffende dienst geboden niveau van gegevensbescherming. Bij de weging wordt dus ook bepaald of er gegevens kunnen worden verstrekt. De gemaakte weging wordt door de minister geaccordeerd. Verstrekking aan buitenlandse diensten vindt vervolgens plaats of in het kader van een goede taakuitvoering (artikel 62) dan wel in het kader van een samenwerkingsrelatie (artikel 89); daarbij kunnen aan de verstrekking voorwaarden worden verbonden (in ieder geval altijd de derde-partijregel). Op dit proces – van begin tot eind – vindt toezicht plaats door de afdeling toezicht van de CTIVD. Het toezicht door de afdeling toezicht is (inhoudelijk en qua bevoegdheden) op relevante aspecten vergelijkbaar met dat van de IC Commisioner en de klachtbehandeling door de afdeling klachtbehandeling met dat van de IPT.

vi. Bij de bespreking van de zesde eis blijkt dat in het VK er blijkbaar de plicht bestaat voor de Secretary of State om een last (*warrant*) in te trekken (ook voor de datum waarop deze afloopt), indien die niet langer noodzakelijk is. (ov. 400)

De Wiv 2017 kent niet de mogelijkheid tot het intrekken van een last. In algemene zin geldt op grond van artikel 26, vierde lid, wel dat de uitoefening van een bevoegdheid onmiddellijk wordt gestaakt, indien het doel waartoe de bevoegdheid is uitgeoefend is bereikt, dan wel met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan. Hierop kan door de CTIVD toezicht worden gehouden.

Waar het gaat om de door de (desbetreffende) Britse inlichtingendienst gehanteerde bewaartermijn van ontvangen ruwe (*unanalysed*) geïntercepteerde gegevens, zowel inhoud als gerelateerde *communications data*, moet men voor de verschillende categorieën van gegevens maximum bewaartermijnen vaststellen – overeen te komen met de IC Commisioner - waarbij rekening moet worden gehouden met de aard en ingrijpendheid van die gegevens. Gemiddeld geldt een maximum van twee jaar voor ruw materiaal; daarna vernietiging.

Materiaal dat niet met een *strong selector* is uitgeselecteerd wordt direct vernietigd; indien op dat materiaal ook een *complex query* wordt toegepast mag het een paar dagen langer worden bewaard, maar indien niet geselecteerd, wordt de data terstond vernietigd. Geselecteerd materiaal wordt vervolgens na zes maanden automatisch vernietigd, tenzij gebruikt in onderzoek. Alleen in exceptionele gevallen kan verlenging plaatsvinden. Wel stelt het Hof vast dat de toegepaste bewaartermijnen significant korter zijn dat de genoemde twee jaar. (ov. 402-403). Het Hof zegt overigens niets over hoe lang of kort een termijn zou mogen/moeten zijn. Wel geeft het Hof aan dat – in plaats van (kortgezegd) de vastlegging ervan in "*above the waterline arrangements*" – dergelijke termijnen idealiter in wetgeving worden vastgelegd (*legislative and/or other general measures*). (ov. 405)

vii. *Supervision* (de zevende eis) – toezicht – wordt in het VK uitgeoefend door de IC Commissioner, waarbij overigens door het Hof wordt benadrukt dat er ook een belangrijke rol is weggelegd voor de staf en de juristen binnen de intercepterende dienst (*intercepting agency*;) of het ministerie dat de *warrant* verleent in de vorm van onafhankelijk advies en pre-autorisatie-toets. De IC Commisioner – als men de beschrijving van zijn taak, functie en bevoegdheden beziet – is als instantie grotendeels vergelijkbaar met de afdeling toezicht van de CTIVD (ov. 407). Tot diens taak behoort ook toezicht op het delen van geïntercepteerd materiaal met partnerdiensten (*intelligence partners*). (ov. 411). Het Hof concludeert – alles overziend – dat de IC Commissioner onafhankelijk en effectief toezicht op het bulkinterceptieproces houdt. (ov. 412) Van bindende oordeelsvorming door de IC Commissioner is geen sprake.

viii. Ex post facto review – achtste eis – vindt in het VK plaats door het IPT (Investigatory Powers Tribunal).

In dit kader is het goed om op te merken dat bij de voorbereiding van het voorstel voor de (uiteindelijke) Wiv 2017 de uitspraak van het EHRM in de Kennedy-zaak waar het gaat om de inrichting van het bindend klachtstelsel in de wet richtinggevend is geweest; voor de afdeling klachtbehandeling heeft het IPT model gestaan; een aantal aspecten, zoals de mogelijkheid van publieke hoorzittingen (tenzij…), de bevoegdheid tot het toekennen van schadevergoeding is niet overgenomen. De IPT is aan te merken als een rechterlijke instantie (*independent court*), die specifiek in het leven is geroepen teneinde te bewerkstelligen dat het VK aan zijn verplichtingen ex artikel 13 EVRM kan voldoen. De afdeling klachtbehandeling van de CTIVD is te kwalificeren als semi-rechterlijk.

15. Met inachtneming van het hiervoor in paragraaf 13 gestelde, beziet het Hof vervolgens de problematiek van (aan de inhoud van communicatie) gerelateerde verkeersgegevens (*related communications data*). (ov. 416 e.v.) In dat kader – voor zover relevant voor het Nederlandse stelsel – kan het volgende worden genoteerd:

i. Nu in het VK de in het kader van het toepasselijke wettelijke interceptieregime te verlenen *warrants* zowel de interceptie van inhoud als *related communications* betreffen en de *related communications data* op een (vrijwel) identieke manier worden behandeld, treft het oordeel inzake de tekortkomingen van het Britse stelsel met betrekking tot de inhoud ook die andere gegevens. Ergo: de afwezigheid van onafhankelijke autorisatie (vooraf); het niet opnemen van categorieën van selectoren in een *warrant*; het ontbreken van interne autorisatieprocedure met betrekking tot selectoren die gelinkt zijn aan identificeerbare personen en het gebrek aan voorzienbaarheid van de omstandigheden waarin *communications* kunnen worden onderzocht.

Bij de interceptie op grond van artikel 48 Wiv 2017 wordt geen onderscheid gemaakt naar inhoud en verkeersgegevens; beide worden gelijktijdig geïntercepteerd. Het onderscheid wordt pas relevant bij de verdere verwerking (artikel 50). Deze verdere verwerking (selectie en metadata-analyse) is onderworpen aan onafhankelijke "autorisatie", dat wil zeggen

bindende ex ante toets door TIB. Zie omtrent de selectiebevoegdheid, hetgeen hiervoor daaromtrent is opgemerkt.

ii. Het Hof stelt vast dat veel van de gehanteerde werkwijzen en procedures hetzelfde zijn bij zowel inhoud als *related communications data*, maar op twee principiële wijzen behandelt het bulkinterceptieregime inhoud en *related communications data* verschillend: (1) het gebruik van selectoren met betrekking tot personen die "*in the British Islands*" verblijven (binnenlands verkeer) en (2) het feit dat *related communications data* die niet via een *strong selector* of een *complex query* werden geselecteerd niet direct worden vernietigd, maar voor enkele maanden worden bewaard.

Het eerste aspect is nauw verweven met de inrichting van het Britse stelsel (onderscheid binnen- en buitenlands verkeer, dat Nederland niet kent) en blijft hier verder buiten beschouwing. Het tweede aspect is voor het Nederlandse stelsel mogelijk wel relevant; zie hierna.

iii. Met betrekking tot het tweede aspect is – omdat dat ook in de Nederlandse discussie een rol speelt – het goed om de overwegingen van de Britse regering (zoals weergeven door het Hof) te noemen, waarom een langere termijn noodzakelijk is: "*As for the duration of storage, the Government contendend that related communications data "require more analytical work, over a lengthy period, to discover 'unknown unknowns' ". That discovery could involve an exercise of piecing together disparate small items of communications data to form a "jigsaw" revealing a threat, and would include the possible examination of items that initially appeared to be of no intelligence interest. Discarding unselected communications data immediately, or even after a few days, would render that exercise impossible".* Het Hof accepteert deze langere bewaartermijn, omdat er sprake is van een maximum bewaartermijn die – aldus het Hof – "*dit not exceed "several months"* "en het verschil in behandeling van inhoud en *related communications data* objectief en redelijk is gerechtvaardigd. Wel acht het Hof noodzakelijk dat vanuit de eis van voorzienbaarheid die bewaartermijn opgenomen dient te zijn in "*appropriate legislative and/or other general measures*".

Hoewel het Hof zich niet over een specifieke bewaartermijn heeft uitgelaten betrekt het Hof in zijn oordeelsvorming wel nadrukkelijk dat deze termijn (slechts) enkele maanden betreft.

<u>B. De ontvangst van gegevens/materiaal van buitenlandse inlichtingendiensten</u>.

16. Een specifiek aan het Hof voorgelegde kwestie betreft de <u>ontvangst</u> door autoriteiten van het VK van materiaal van buitenlandse inlichtingendiensten, in het bijzonder van de Amerikaanse dienst NSA (toepassing van de programma's Upstream en PRISM).

17. De allereerste kwestie waar het Hof zich over buigt is die van de toepasselijkheid van het EVRM (*applicable test*). In dat kader geeft het Hof allereerst de opvatting van de Kamer weer (die door het Hof wordt onderschreven): interceptie van communicatie door een buitenlandse dienst kan <u>niet</u> leiden tot verantwoordelijkheid van de ontvangende Staat, of binnen de jurisdictie van die Staat vallen zoals bedoeld in artikel 1 van het EVRM, <u>zelfs als de interceptie op verzoek van die Staat heeft plaatsgevonden</u>. Volgens vaste jurisprudentie van

het Hof valt de interceptie van communicatie door een buitenlandse inlichtingendienst alleen binnen de jurisdictie van de ontvangende Staat indien die Staat gezag/macht (*authority*) of controle over die dienst uitoefent.

> **Dit is een belangrijke notie bij de uitleg van artikel 90, lid 3, Wiv 2017. Artikel 90, lid 3, ziet op het doen van een verzoek aan een buitenlandse dienst tot het verrichten van handelingen die overeenkomen met de uitoefening van een bijzondere bevoegdheid. Indien de buitenlandse dienst een dergelijk verzoek honoreert, wordt dat door die buitenlandse dienst uitgevoerd binnen diens jurisdictie en conform de regels die voor die dienst gelden. De Nederlandse dienst kan niet verantwoordelijk worden gehouden voor de uitvoering.**

Het Hof is het met de Kamer eens dat dit in de voorliggende casus niet aan de orde is. *"Therefore, any interference with Article 8 of the Convention could only lie in the initial request and the subsequent receipt of intercept material, followed by its subsequent storage, examination and use by the intelligence services of the receiving State"*. (ov. 496). Het Hof stelt voorts: *"The protection afforded by the Convention would be rendered nugatory if States could circumvent their Convention obligations by requesting either the interception of communications by, or the conveyance of intercepted communications from, non-Contracting States; or even, although not directly in issue in the cases at hand, by obtaining such communications through direct access to those States' databases."(*ov. 497)

> **Het Hof stelt vast dat een inmenging met 8 EVRM wel aanwezig kan zijn bij het doen van het initiële verzoek (om interceptie) aan een buitenlandse dienst en de verdere verwerking van ontvangen materiaal als gevolg van de (gevraagde) interceptie. De bescherming die door het EVRM wordt geboden zou (anders) van zijn betekenis worden ontdaan indien men de verplichtingen van het EVRM kan omzeilen via het doen van verzoeken aan Staten die geen partij zijn bij het EVRM (zoals in casu de VS). Voor Staten die wel partij zijn bij het EVRM geldt immers dat men EVRM-conform dient te handelen.**

18. Het Hof stelt vervolgens aan een verzoek aan een *non-contracting State* (niet bij EVRM aangesloten Staat, zoals de VS) om geïntercepteerd materiaal de volgende eisen:
    i. Het verzoek moet een grondslag hebben in het nationale recht;
    ii. De wet moet toegankelijk zijn voor de personen die het betreft en voorzienbaar in zijn gevolgen;
    iii. Voorts moeten er heldere gedetailleerde regels zijn die de burgers een adequate indicatie geven van de omstandigheden waarin en de voorwaarden waaronder de autoriteiten een dergelijk verzoek mogen doen en die voorzien in effectieve waarborgen tegen het gebruik van de bevoegdheid om daarmee nationaal recht en/of de verplichtingen van de Staat onder het EVRM te omzeilen. (ov. 497)

19. Vanaf het moment dat het geïntercepteerde materiaal wordt ontvangen, dient de ontvangende Staat, aldus het Hof, adequate waarborgen voor het onderzoek, gebruik en de opslag ervan te hebben (*to have in place*); idem voor de doorverstrekking; en voor de verwijdering en vernietiging. Deze waarborgen, die door het Hof in eerste instantie zijn ontwikkeld in zijn jurisprudentie met betrekking tot de interceptie van communicatie door de bij het EVRM aangesloten Staten, zijn gelijkelijk van toepassing op de ontvangst, door een aangesloten Staat, van gevraagd interceptiemateriaal (*solicited intercept material*) van een buitenlandse inlichtingendienst. Indien, zoals in casu door het VK is aangevoerd, niet altijd

duidelijk is of het ontvangen materiaal het resultaat is van interceptie, dan dienen, aldus het Hof, dezelfde standaarden van toepassing te zijn met betrekking tot al het materiaal ontvangen van een buitenlandse inlichtingendienst dat het product van interceptie kan zijn. Dit laatste lijkt erop te duiden dat als het ontvangen materiaal voldoet aan de kenmerken van geïntercepteerd materiaal het ook als zodanig dient te worden behandeld.

In de Wiv 2017 is geen expliciete wettelijke grondslag opgenomen voor het mogen vragen van gegevens, waaronder gegevens uit bulkinterceptie, aan buitenlandse diensten. Dat geldt wel voor het vragen van technische en andere vormen van ondersteuning (artikel 90). Het omgekeerde – verstrekking van gegevens en verlenen van technische en andere vormen van ondersteuning – is wel in de wet (artikel 89) geregeld. Het verdient aanbeveling om alsnog in een grondslag voor het vragen van gegevens te voorzien.

In de Wiv 2017 is nog geen expliciete regeling opgenomen, waarbij de waarborgen die gelden voor de verdere verwerking van geïntercepteerd materiaal uit eigen interceptie, ook gelden indien het gaat om geïntercepteerd materiaal dat desgevraagd van een buitenlandse dienst - van een Staat die wel of niet partij is bij het EVRM - wordt ontvangen. De wet zal hierop moeten worden aangepast.

20. Tot slot stelt het Hof als eis dat ieder regime dat aan inlichtingendiensten de mogelijkheid biedt om een verzoek te doen tot interceptie of tot het ontvangen van geïntercepteerd materiaal van een Staat die niet is aangesloten bij het EVRM, of waarbij sprake is van directe toegang tot dergelijk materiaal, dit onderworpen dient te zijn aan onafhankelijk toezicht en de mogelijkheid van een onafhankelijk ex post review. (ov. 499)

C. Artikel 10 EVRM en bulkinterceptie

21. Het Hof heeft zich in zijn uitspraak ook gebogen over de toepassing van artikel 10 EVRM in de context van bulkinterceptie. Bij de kwesties die aan het EHRM zijn voorgelegd waar het gaat om toepassing van artikel 10 in relatie tot de activiteiten van journalisten gaat het vooral over de bescherming van journalistieke bronnen. In de uitspraak geeft het Hof de algemene principes die ter zake gelden weer (ov. 442-445). De in de jurisprudentie van het Hof ontwikkelde eis van een voorafgaande bindende toets waar het gaat om de verwerving van gegevens die zicht kunnen geven op bronnen van journalisten, is in de Wiv 2017 gecodificeerd. Zo is in artikel 30, tweede lid, van de Wiv 2017 vastgelegd dat de voor de uitoefening van bijzondere bevoegdheden op journalisten, waarbij de uitoefening kan leiden tot verwerving van gegevens inzake de bron van de journalist, toestemming van de rechtbank Den Haag is vereist.

22. In de uitspraak gaat het Hof specifiek in op de betekenis van artikel 10 EVRM in de context van bulkinterceptie. Ingeval van bulkinterceptie kan vertrouwelijk journalistiek materiaal door de diensten zowel doelgericht (bijvoorbeeld door toepassing van daarop gerichte selectoren) of als "bijvangst" in het kader van de bulkinterceptie-operatie worden verworven. Waar het gaat om een doelgerichte activiteit (*intention to access*) van de diensten om vertrouwelijk journalistiek materiaal te verwerven merkt het Hof het volgende op: *"Therefore, the Court considers that before the intelligence services use selectors or search terms known to be connected to a journalist, or which would make the selection of confidential journalistic material for examination highly probable, the selectors or search*

terms must have been authorized by a judge or other independent and impartial decision-making body invested with the power to determine whether they were "justified by an overriding requirement in the public interest" and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest (…)". (ov. 448)

> **In artikel 30, tweede lid, Wiv 2017 is bepaald dat de uitoefening van een bijzondere bevoegdheid jegens een journalist, waarbij de uitoefening kan leiden tot verwerving van gegevens inzake een bron van een journalist, slechts is toegestaan, indien de rechtbank Den Haag, op verzoek van de betrokken minister, daartoe toestemming heeft verleend. Dat geldt dus ook voor de uitoefening van de bevoegdheid ex artikel 50, eerste lid, onder a, van de wet. Wel zal in het verzoek om toestemming in dit soort gevallen de selectoren of zoektermen (specifiek) dienen te worden opgenomen.**

In de tweede situatie, waarbij geen sprake is van een doelgerichte activiteit om vertrouwelijk journalistiek materiaal te verwerven, bestaat er – aldus het Hof - niettemin een risico dat dergelijk materiaal kan worden geïntercepteerd, en zelfs kan worden onderzocht, als "bijvangst" van de bulkinterceptie-operatie. Naar het oordeel van het Hof is een dergelijke situatie in materiële zin afwijkend ten opzichte van de situatie van een gericht onderzoek van een journalist (*targeted surveillance of a journalist*). Immers, anders dan bij een gericht onderzoek, kan het bij bulkinterceptie altijd voorkomen dat (ook) dergelijk materiaal wordt geïntercepteerd. Dat is op voorhand vaak niet te voorzien, zodat het in de autorisatiefase voor een rechter of een ander onafhankelijk lichaam niet mogelijk is om te beoordelen of een dergelijke inmenging met het in artikel 10 EVRM gegarandeerde recht wordt gerechtvaardigd door een "*overriding requirement in the public interest*" en, meer in het bijzonder, of met een minder ingrijpende maatregel had kunnen worden volstaan. Het Hof komt thans echter tot een andere lijn, dan eerder gehanteerd in de zaak Weber en Saravia tegen Duitsland, waarbij in een dergelijke situatie werd aanvaard dat er geen sprake was van een ernstige inmenging met artikel 10 EVRM. Het Hof stelt thans: *"Nevertheless, (…), in the current, increasingly digital, age technological capablilities have greatly increased the volume of communications traversing the global internet, and as a consequence surveillance which is not targeted directly against individuals has the capacity to have a very wide reach indeed, both within and without the territory of the surveilling State."*(ov. 450) Het Hof geeft vervolgens aan dat nu het onderzoek van de communicatie of de gerelateerde verkeersgegevens van een journalist door een analist kan leiden tot de identificatie van een bron, het nationale recht moet voorzien in een robuuste waarborgen betreffende opslag, onderzoek, gebruik, verdere verstrekking en vernietiging van dergelijk vertrouwelijk materiaal. Aansluitend stelt het Hof dat – buiten de situatie van toepassing van gerichte selectie of gerichte zoektermen – er voor het geval dat het duidelijk wordt dat het geïntercepteerde materiaal (communicatie en gerelateerde verkeersgegevens) vertrouwelijk journalistiek materiaal bevat, de voortdurende opslag en onderzoek van dat materiaal door een analist (*their continued storage and examination by an analyst*) alleen mogelijk is indien dit is geautoriseerd door een rechter of een ander onafhankelijke en onpartijdige besluitvormend lichaam (*decision-making body*) die kan beslissen of de voortdurende opslag en het onderzoek wordt gerechtvaardigd door een "*overriding requirement in the public interest*". (ov. 450)

> **Deze nieuwe eis van het Hof vereist aanpassing van de Wiv 2017, aangezien de wet daarin nog niet voorziet. Te overwegen is (ook) deze toestemming te beleggen bij de rechtbank Den Haag. Wel zal in afwachting van een wettelijke voorziening ter zake dienen te worden bezien hoe – bij wijze van een tijdelijke voorziening – de geëiste toestemming kan worden georganiseerd.**

Centrum för Rättvisa tegen Zweden

1. In deze zaak staat ook bulkinterceptie voor nationale veiligheidsdoeleinden centraal. Het door het Hof in het kader van de Big Brother Watch-zaak gepresenteerde (nieuwe) normenkader voor de beoordeling of een bulkinterceptieregime verdragsconform is, wordt in deze zaak ook toegepast; zie daartoe ov. 236-278. Voor de bijzonderheden daarvan wordt verwezen naar hetgeen hiervoor daaromtrent is opgenomen bij de Britse zaak. In het onderstaande zal louter nog worden ingegaan op de toepassing van dat normenkader op het Zweedse regime voor bulkinterceptie – dat uitsluitend betrekking heeft op "*cross border*" communicatie (oorsprong of bestemming in het buitenland en dus niet binnenlands verkeer) – voor zover de door het Hof gegeven overwegingen ook van belang (kunnen) zijn voor de Nederlandse situatie. Een verschil tussen de Zweedse zaak en de Britse zaak is ten slotte, dat hier de verstrekking van gegevens uit bulkinterceptie aan buitenlandse diensten door het Hof wordt getoetst.

2. In de Zweedse zaak staat met name de vraag centraal of het nationale recht toegankelijk was en adequate en effectieve waarborgen en garanties bevatte om te voldoen aan de uit artikel 8 EVRM voortvloeiende eisen van "voorzienbaarheid" en "noodzakelijk in een democratische samenleving". Daarbij wordt gelijktijdig naar zowel de inhoud van de communicatie als de *related communications data* (verkeersgegevens) gekeken, nu in de Zweedse wetgeving ter zake dezelfde wettelijke voorzieningen, procedures en waarborgen betreffende de interceptie, bewaren, onderzoek, gebruik en opslag van elektronische signalen van toepassing zijn zonder dat er onderscheid wordt gemaakt tussen *communications data* en de inhoud van communicatie. (ov. 283) Daartoe onderzoekt het Hof of het Zweedse stelsel aan de acht door het Hof geformuleerde eisen voldoet.

3. Voorafgaand daaraan is het goed om in het kort uiteen te zetten welke procedure door de Zweedse dienst (FRA) moet worden bewandeld om over te kunnen gaan tot bulkinterceptie en welke rol bepaalde instanties daarin spelen. Volgens de Zweedse wet moet iedere "*signals intelligence mission*" uitgevoerd door FRA van te voren te worden geautoriseerd door de Foreign Intelligence Court (een onafhankelijke rechterlijke instantie, met bindende bevoegdheden; FIC). In een verzoek om toestemming moet de behoefte aan de benodigde gegevens (*intelligence sought*), de dragers van communicatie waartoe men toegang wil krijgen en de selectoren die betrekking hebben op identificeerbare personen – althans op zijn minst de categorie van selectoren – te worden benoemd. Dit wordt door het FIC onder meer op proportionaliteit getoetst. In spoedgevallen mag FRA zonder een dergelijke voorafgaande toestemming zichzelf toestemming geven om overgaan tot interceptie, maar moet dit terstond bij deze instantie melden die het dan met spoed moet bezien en de macht heeft om de toestemming in te trekken of aan te passen. Naast het FIC is er voorzien in een toezichthouder, de Foreign Intelligence Inspectorate. Deze heeft verstrekkende bevoegdheden die zien op de gehele keten van SIGINT-activiteiten. Een belangrijke taak is het verlenen van toegang van FRA (*granting FRA access*) tot de communicatiedragers nadat ze hebben beoordeeld of de door FRA verzochte toegang overeenkomt met de eerder door het FIC verleende toestemming.

4. In het kader van het onderzoek of aan de tweede eis wordt voldaan, gaat het Hof ook in op de mogelijkheid van de Zweedse dienst (FRA) om ten behoeve van ontwikkeldoeleinden (*development activities*) signalen te intercepteren. *"It is true that the FRA may also intercept signals as part of its development activities, which may lead to data not relevant for the*

regular foreign intelligence being intercepted. (…) that signals intercepted as part of the FRA's development activities can be used, including by being "read" and stored, for technological development purposes regardless of whether they fall within the categories defined under the eight foreign intelligence purposes" (ov. 291). Het Hof stelt vast dat bij de door FRA in die context geïntercepteerde signalen de autoriteiten niet geïnteresseerd zijn in de inhoud ervan maar alleen voor de mogelijkheid die ze bieden ten behoeve van de analyse van de systemen en de routes waarlangs informatie wordt overgebracht. In dat kader verwijst naar door de Zweedse overheid aangedragen voorbeelden, zoals onder meer het monitoren van het verkeer tussen bepaalde landen met het oog op het identificeren van dragers met relevant verkeer. Ter zake concludeert het Hof: *"The degree of interference with individuals' Article 8 rights engendered by such activities appears to be of a very low intensity having regard to the fact that the data thereby obtained is not in a form destined to generate intelligence."* (ov. 291-292). Voor het uitvoeren van een dergelijke activiteit behoeft de FRA overigens wel een toestemming van de "*Foreign Intelligence Court*" en wordt er toezicht uitgeoefend door het *Inspectorate*.

De Wiv 2017 voorziet in een (deels) vergelijkbare bevoegdheid in artikel 48, eerste lid, zij het inherent aan een geaccordeerde bevoegdheid tot OOG-interceptie, en artikel 49, eerste lid. Daarvoor is naast toestemming van de minister ook een bindende rechtmatigheidstoets van de TIB vereist.

5. Bij de beoordeling van de derde eis – namelijk de procedure die moet worden gevolgd voor het verlenen van autorisatie voor bulkinterceptie -, waarbij het eerder genoemde *Foreign Intelligence Court* een belangrijke rol speelt, wordt vastgesteld dat FRA ingeval men toestemming aanvraagt niet alleen de noodzaak moet aantonen voor de gegevens die men wil verwerven (*intelligence sought*), de gegevensdragers waartoe men toegang wenst te verkrijgen maar ook de selectoren – of op zijn minst de categorie van selectoren – die men wil gebruiken. Het Hof geeft in de slotoverweging bij dit onderdeel nogmaals aan waar het bij de toets aan deze eis over gaat: *"However, for the purposes of the Court's analysis, at this stage the relevant point is that the Swedish authorisation system offers a judicial ex ante review of permit requests which is comprehensive, in the sense that the aim of the mission and the bearers and categories of selectors to be used are subject to control, and is sufficiently detailed in respect of secret bulk signals intelligence as part of foreign intelligence. Such a review offers a significant safeguard against, notably, the launch of abusive or clearly disproportionate bulk interception operations. Importantly, it also sets the framework within which a concrete operation must unfold and the limits whose observance then becomes the object of the applicable supervision and ex post facto control mechanisms."* (ov. 302).

Zoals reeds in het kader van de bespreking van de Britse zaak is vastgesteld voldoet het in de Wiv 2017 neergelegde stelsel voor het verlenen van goedkeuring voor OOG-interceptie (artikel 48) aan de door het Hof gestelde eisen, zij het dat waar het gaat om de voorafgaande autorisatie van de categorieën van selectoren (artikel 50) de wet aanpassing behoeft om dat nadrukkelijk vast te leggen. In de praktijk wordt al EVRM-conform gehandeld, waarbij het aangewezen is dit in een beleidsregel vast te leggen.

6. Bij de beoordeling of wordt voldaan aan de vierde eis – namelijk de procedures die moeten worden gevolgd voor selecteren, onderzoek en gebruik van geïntercepteerd materiaal –

merkt het Hof op dat de verplichting om loggings en gedetailleerde verslagen bij te houden van iedere stap in bulk interceptie operaties, met inbegrip van de gebruikte selectoren, in nationaal recht geregeld dient te zijn. Een regeling ter zake (louter) in interne instructies, zoals in Zweden, wordt als een tekortkoming aangemerkt. (ov. 311). Het bestaan van overall toezicht op de activiteiten van FRA – en dus ook op de plicht tot bijhouden loggings e.d. – lijkt dit gebrek te compenseren.

In artikel 31 van de Wiv 2017 wordt in algemene zin geregeld dat van de uitoefening van een bevoegdheid aantekening wordt gehouden. Daaronder – in combinatie met de zorgplicht ex artikel 24 van de wet – valt ook de logging van de handelingen in het kader van OOG-interceptie operaties. Voor de gehanteerde selectoren biedt artikel 50, derde lid, een regeling. Op een en ander ziet de CTIVD toe.

7. Bij de beoordeling van <u>de vijfde eis</u> – de voorzorgen die genomen moeten worden wanneer er materiaal (gegevens) aan andere partijen worden verstrekt – besteedt het Hof in het bijzonder aandacht aan de mogelijkheid tot het verstrekken van gegevens (*intelligence*) aan buitenlandse partijen (ondanks het feit dat er geen concrete verstrekking aan de orde was gesteld); bij de behandeling voor de gewone Kamer waren bij deze wel zorgen ter zake gerezen, maar men ging er uiteindelijk van uit dat via het toezichtsmechanismen op voldoende wijze tegenwicht zou worden geboden aan tekortkomingen in de regelgeving op dat vlak (*counterbalance these shortcomings*). Het Hof: *" Nonetheless, insofar as the possibility of transmitting intelligence to foreign parties is part of the Swedish bulk interception regime and activities whose very existence can be seen as interfering with Article 8 rights, the Court, having regard to the applicant's complaints, must review the Swedish intelligence transmission regime and its functioning for their compliance with the requirements of quality of the law and necessity in a democratic society."* (ov. 320) Het gaat hier – anders dan in de Britse zaak – <u>uitsluitend om de verstrekking aan buitenlandse partijen</u>. In dit kader geeft het Hof aan dat het niet ter discussie staat dat bij het EVRM aangesloten Staten aan buitenlandse diensten gegevens moeten verstrekken die zijn verkregen door bulkinterceptie van communicatie vanwege verschillende redenen, zoals het waarschuwen tegen dreigingen e.d. Internationale samenwerking is – aldus het Hof – cruciaal voor de effectiviteit van de inspanningen van autoriteiten om mogelijke dreigingen tegen de nationale veiligheid te ontdekken en tegen te gaan. (ov. 321) Het Hof erkent dat de precieze reikwijdte van het delen van gegevens niet in de wet kan worden omschreven (bijvoorbeeld via een opsomming van de situaties waarin of de soorten gegevens die verstrekt mogen worden). De toepasselijke wetgeving (*legal regulation*) en praktijk moet echter wel op zodanige wijze werken dat daarmee het risico op misbruik en disproportionele inmenging van de in artikel 8 EVRM gegarandeerde rechten wordt beperkt. Allereerst dienen de gegevens die aan buitenlandse diensten worden verstrekt en zijn verkregen via bulkinterceptie het product te zijn van wettelijk geregelde procedures waarop alle relevante waarborgen van toepassing zijn. Indien het gaat om gegevens die via deze wijze zijn verkregen, wordt daarmee ook – op zijn minst tot op zekere hoogte – het risico op nadelige gevolgen die nadat verstrekking aan een buitenlandse partner heeft plaatsgevonden kunnen optreden, beperkt.

In het kader van de (parlementaire) behandeling van de Wiv 2017 is de eis dat bij de verstrekking van gegevens aan buitenlandse diensten het moet gaan om

rechtmatig verworven gegevens als een van de (vier) sleutels op de deur voor samenwerking gekenschetst.

Het Hof stelt voorts vast dat het ontbreken van een uitdrukkelijke wettelijke eis voor de FRA om de noodzakelijkheid en proportionaliteit van het delen van gegevens (*intelligence sharing*) op de mogelijke impact op het door artikel 8 EVRM gegarandeerde recht te beoordelen, een substantiële tekortkoming vormt van het Zweedse regime voor bulkinterceptie-activiteiten. Ook stelt men vast dat de Zweedse dienst niet verplicht is actie te ondernemen in gevallen waarin, bijvoorbeeld, gegevens die ernstige inbreuk op privacyrechten maken aanwezig zijn in het materiaal dat naar het buitenland wordt verzonden zonder dat er sprake is van enige significante "*intelligence value*". Voorts, aldus het Hof, ondanks het feit dat de Zweedse autoriteiten duidelijk controle verliezen over de met een buitenland gedeelde gegevens zodra deze zijn verzonden, bestaat er geen wettelijke verplichting voor de FRA om te analyseren en te bepalen of er bij de buitenlandse ontvanger een acceptabel minimum niveau van waarborgen aanwezig is. Het antwoord van de Zweedse regering dat samenwerking met buitenlandse diensten onvermijdelijk functioneert op basis van een gedeeld belang in het bewaren van de geheimhouding van de informatie en dat dit in de praktijk de risico op misbruik beperkt, acht het Hof ontoereikend. De aldus geschetste benadering acht het Hof dan ook een onvoldoende waarborg. Anders dan de Kamer is het Hof van oordeel dat deze gebreken niet op voldoende wijze kunnen worden gecompenseerd (*sufficiently counterbalanced*) door het in het Zweedse regime neergelegde stelsel van toezicht. Dit gebrek zal dan ook door het Hof worden meegewogen bij de vraag of sprake is van overeenstemming met artikel 8 EVRM.

De Wiv 2017 kent deze gebreken niet. Voor alle vormen van gegevensverwerking, dus ook de verstrekking aan buitenlandse diensten gelden de in artikel 18 neergelegde eisen (doelbinding, noodzakelijkheid, zorgvuldig en behoorlijk) waarbij de eisen van proportionaliteit en subsidiariteit thans onder het criterium behoorlijk worden geschaard. Voorts geldt dat voor de samenwerking met buitenlandse diensten wegingsnotities moeten worden opgesteld waarin de door het Hof genoemde aspecten worden betrokken (artikel 88).

8. In het kader van de zesde eis – beperkingen aan de duur van de interceptie, de opslag van geïntercepteerde gegevens en de omstandigheden waarin dergelijke gegevens moeten worden gewist en vernietigd – merkt het Hof, waar het gaat om de duur van de interceptie, op, dat het op zich aan de nationale autoriteiten is om die duur te bepalen. Wel stelt men dat er adequate waarborgen moeten zijn, zoals een duidelijke indicatie in de wet na welke periode een last (*warrant*) afloopt, de voorwaarden waaronder deze kan worden verlengd en de omstandigheden waaronder de last moet worden ingetrokken. (ov. 331) Bij dit laatste aspect staat het Hof wat langer stil. *" The Court is of the view that an express provision on discontinuation of bulk interception when no longer needed would have been clearer than the existing arrangement in Sweden according to which, apparently, permits may or may not be cancelled when circumstances warranting such a cancellation came to light in the period before the expiry of their six months' validity."* (ov. 335) *"The significance of this shortcoming should however, not be overestimated, in the Court's view, (…)" "(…), in the specific context of bulk interception for foreign intelligence purposes, the existence of supervision mechanisms with access to all internal information must generally be seen as providing similar legislative safeguards against abuse related to the duration of interception operations."* (ov. 336)

De Wiv 2017 kent niet de mogelijkheid tot het intrekken van een last. In algemene zin geldt op grond van artikel 26, vierde lid, wel dat de uitoefening van een

bevoegdheid onmiddellijk wordt gestaakt, indien het doel waartoe de bevoegdheid is uitgeoefend is bereikt, dan wel met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan. Hierop kan door de CTIVD toezicht worden gehouden.

9. Waar het gaat om de vernietiging van geïntercepteerd materiaal, waarbij wordt vastgesteld (primair door de Kamer) dat er diverse bepalingen bestaan die de situaties regelen waarin gegevens moeten worden vernietigd, wijst het Hof erop dat *"(…), while there is a clear justification for special requirements regarding the destruction of material containing personal data, there must also be a general legal rule governing the destruction of other material obtained through bulk interceptions of communications, where keeping it may affect, for example the right of respect for correspondence under Article 8, including concerning legal persons as the applicant. As a very minimum (…) there should be a legal requirement to delete intercepted data that has lost pertinence for signals intelligence purposes."* (ov. 342)

10. De zevende door het Hof geformuleerde eis betreft het toezicht op het bulkinterceptie regime: "*The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance".* Het toezicht is in Zweden hoofzakelijk toebedeeld aan de *Foreign Intelligence Inspectorate*. Daarnaast bestaan ook nog andere toezichthoudende instanties, zij het met minder bevoegdheden, zoals de DPA. Het *Inspectorate* kan volgens het Hof als een onafhankelijk controlemechanisme worden aangemerkt. Het Hof omschrijft vervolgens de bevoegdheden van dit *Inspectorate*, die hier integraal worden weergegeven mede in verband met de discussie over de wenselijkheid van integratie van de taken en bevoegdheden van de TIB in de CTIVD. *"The Inspectorate has wide-ranging powers covering the operation of signal intelligence activities from beginning to end. In particular, it is tasked with granting the FRA access to communication bearers after verifying that the requested access corresponds to the permit issued by the Foreign Intelligence Court (…). The Inspectorate reviews all other aspects of the FRA's activities, including the interception, analysis, use and destruction of material. Importantly, it can scrutinize the selectors used (…) and enjoys access to all relevant documents of the RA (…).."* (ov. 347)

    In (het vervolg van) de uitspraak komt het Hof niet terug op het feit dat een en dezelfde instantie de bevoegdheid heeft om bindend te bepalen of FRA daadwerkelijk toegang krijgt tot de dragers (bijvoorbeeld kabels) en vervolgens over het hele traject – dus inclusief voornoemd onderdeel - toezicht uitoefent en blijkbaar vindt het Hof dat (dus) geen probleem. Hoewel het verlenen van toegang tot de dragers niet geheel hetzelfde is als hetgeen de TIB doet met betrekking tot verleende toestemmingen door de minister, lijkt er geen principieel bezwaar te zijn om de taken en bevoegdheden van de TIB te combineren met die van de afdeling toezicht van de CTIVD. Zelfs zonder Chinese muren. Wel is aandachtspunt dat in het Zweedse stelsel de initiële last (warrant) om überhaupt bulkinterceptie te kunnen verrichten wordt verleend door een onafhankelijke rechter (de FIC). Daar is in Nederland geen sprake van.

    Het Hof staat vervolgens stil bij de bevoegdheden van het *Inspectorate*. Waar het gaat om bulkinterceptie komt het Inspectorate de bindende bevoegdheid toe om ingeval dat men bewijs vindt dat er sprake is van een onbehoorlijke verwerving van Sigint men deze verwerving kan doen beëindigen en ook kan bepalen dat gegevens moeten worden vernietigd; in bepaalde andere gevallen – zo stelt het Hof vast – kan het *Inspectorate*

bepaalde feiten (zoals bijvoorbeeld het vermoeden dat een bepaald strafbaar feit is gepleegd) aan bevoegde autoriteiten rapporteren die ter zake over bindende bevoegdheden beschikken. Voor het overige kan het *Inspectorate* in het kader van het toezicht aanbevelingen en opinies uitbrengen. Met betrekking tot dit gehele complex komt het Hof tot het volgende oordeel: *"The Court considers the above arrangements to be satisfactory. While it is true that there appears to be no legal possibility under Swedish law for the enforcement of the Inspectorate's recommendations when it seeks the evolution or correction of practices by the FRA, the Court observes that (…) the FRA had routines in place for handling the Inspectorate's opinions, the latter's suggestions were dealt with in a serious manner and, when called for, gave rise to reforms"* (ov. 350) Het Hof stelt vervolgens vast dat het Inspectorate niet alleen in theorie maar ook in de praktijk actief toezicht houdt op de activiteiten van FRA zowel in algemeen systematische zin als per thema. Aan de aanbevelingen en opinies van de Inspectorate wordt vrijwel altijd gevolg gegeven. (ov 351).

Het Inspectorate heeft op enkele specifieke onderdelen de mogelijkheid om bindend in te grijpen, en doet daarnaast aanbevelingen die niet kunnen worden afgedwongen maar waar door FRA wel serieus mee wordt omgegaan. Het Hof neemt hiermee genoegen en stelt dus niet de algemene eis het toezicht over de gehele linie bindend dient te zijn.

Resumerend stelt het Hof vast dat onder de gememoreerde omstandigheden er geen reden is om eraan te twijfelen dat de Zweedse wet een effectief toezicht op sigint activiteiten van Zweden bevat. In aanvulling hierop stelt het Hof ten slotte: *"In the Court's view, the Inspectorate's role, coupled with the judicial pre-authorisation procedure before the Foreign Intelligence Court, form together a functioning safeguard against abuse at the crucial stages of the signals intelligence process – before and during the process of interception, analysis, use and destruction of the information obtained."* (ov. 353)

Ook hieruit blijkt weer dat het Hof het stelsel als geheel beziet en dit ook als geheel weegt bij beantwoording van de vraag of er sprake is van een waarborg tegen misbruik in het interceptieproces.

11. De <u>laatste (achtste) eis</u> waaraan wordt getoetst betreft het stelsel van *ex post review*. Naar de Nederlandse situatie vertaald– zie ook hetgeen is gesteld bij de bespreking van de Britse zaak – komt dit (materieel) overeen met hetgeen de afdeling klachtbehandeling van de CTIVD doet, namelijk het bindend oordelen op klachten. Ook in deze zaak komt het Hof tot het oordeel dat " *(..) a remedy which does not depend on notification to the interception subject could be an effective remedy in the context of bulk interception. (…) However, the absence of a functioning notification mechanism should be counterbalanced by the effectiveness of the remedies that must be available to individuals who suspect that their communications may be intercepted and analysed."* (ov. 355) Het Hof stelt vervolgens vast dat de Zweedse wetgeving (*Signal Intelligence Act*) voorziet in ex post factor review, die is opgedragen aan de *Foreign Intelligence Inspectorate*, waarbij een ieder die meent dat hij door een bulkinterceptie operatie is geraakt, om een onderzoek kan verzoeken. Anders dan in Nederland wordt de klager vervolgens uitsluitend geïnformeerd dat er een onderzoek wordt uitgevoerd, maar niet over de uitkomsten daarvan.
    Vervolgens komt er een belangrijke overweging van het Hof die mogelijk van belang kan zijn in de discussie over <u>wat</u> onder één en hetzelfde dak - lees de CTIVD – kan worden gebracht: *"However, while it is true that the Inspectorate is an independent body, the Court observes that, having regard to that body's duty to supervise and monitor the FRA's activities, which includes taking or authorizing operational decisions such as those concerning access to the signal carriers, use of selectors, analysis, use and destruction of intercept material (see paragraphs 50-53 above), the Inspectorate's additional role of ex post facto review on request from individuals may lead to situations where it will have to assess its own activities*

in supervising bulk interception by the FRA. In the conditions of secrecy, which legitimately characterise the relevant procedures, and failing a legal obligation for the Inspectorate to provide reasons to the individual concerned, there may be doubts as to whether the Inspectorate's examination of individual complaints in such situations affords adequate guarantees of objectivity and thoroughness. It cannot be excluded that the dual role of the Inspectorate may generate conflicts of interest and, therefore, the temptation to overlook an omission or misconduct in order to avoid criticism or other consequences." (ov. 395)
Het duale karakter in de taakstelling van het *Inspectorate*, waarbij sprake kan zijn van een situatie waarbij de slager zijn eigen vlees keurt, en waarbij de klager niet gemotiveerd wordt geïnformeerd over het onderzoek, roept twijfel op of er wel sprake is van adequate garanties voor de objectiviteit en indringendheid van het onderzoek door het *Inspectorate*.

> **In de Wiv 2017 is dit aspect nadrukkelijk onder ogen gezien bij het in een organisatie, de CTIVD, plaatsen van de afdeling toezicht en de afdeling klachtbehandeling. Tussen beide afdelingen is – teneinde vooringenomen klachtbehandeling tegen te gaan – een "Chinese muur" aangebracht. Die bestaat feitelijk uit de wijze waarop de CTIVD organisatorisch is ingericht en de regeling inzake het lidmaatschap van beide afdelingen (artikel 98). Een bepaling à la artikel 99, zevende lid, waarbij is bepaald dat de leden van de beide afdelingen niet tevens lid van de TIB kunnen zijn ontbreekt. Het verdient wellicht aanbeveling om nog eens te bezien of deze "Chinese muur" stevig genoeg is. Zou worden overwogen de taken en bevoegdheden van de TIB bij de CTIVD onder te brengen, dan wordt het hier aan de orde zijnde vraagstuk overigens nog wel prangender en zijn er mogelijk verdergaander maatregelen nodig om de onafhankelijkheid van enerzijds toezicht en anderzijds klachtbehandeling ten opzichte van elkaar duidelijker te positioneren (ook op niveau van ambtelijke ondersteuning).**

Het Hof stelt ter zake van het Zweedse systeem voorts dat *"(…)in the Court's view, a system of ex post facto review that does not produce reasoned decisions in response to complaints submitted by individuals, or at least decisions that contain reasons accessible to security-cleared special counsel, is too dependent on the initiative and perseverance of appointed officials operating away from the public eye. (…) A reasoned decision has the undeniable advantage of providing publicly available guidance on the interpretation of the applicable legal rules, the limits to be observed and the manner in which the public interest and individual rights are to be balanced in the specific context of bulk interception of communications. As noted by the Court in Kennedy (…) the publication of such legal rulings enhanced the level of scrutiny in this area. These observations lead the Court to consider that the above-mentioned features of the Swedish system do not offer a sufficient basis for public confidence that abuse, if the occur, will be unveiled and remedied"* (ov. 361) *"In any event, it is of the view that a legal procedure before an independent body, which in so far as possible offers an adversarial process resulting in reasoned and legally binding decisions, is an essential element of an effective ex post facto review."* (ov. 362)

Het Hof komt dan ook – niet verrassend – tot het oordeel dat – gecombineerd met de eerder geschetste duale rol van het *Inspectorate* – het Zweedse stelsel een tekortkoming kent die meegenomen moet worden bij de beoordeling of aan de eisen van artikel 8 EVRM wordt voldaan.

> **Het in de Wiv 2017 neergelegde klachtstelsel ontbeert de gebreken die het Hof ziet in het Zweedse stelsel. Zie echter wel de kanttekening die hiervoor is gemaakt in het geval dat de TIB bij de CTIVD wordt ondergebracht, met name waar het gaat om de onafhankelijke positie van de afdeling klachtbehandeling.**

12. In de concluderende overwegingen geeft het Hof – ten overvloede - een omschrijving van zijn taak, die nog eens duidelijk maakt dat men het aan het Hof voorgelegde stelsel als geheel op verdragsconformiteit beziet: *"The Court further reiterates that it is not its role to prescribe an ideal model for signals intelligence but rather to review for Convention compliance the existing legal and practical arrangements, which vary conceptually and functionally from one Contracting Party to another. In this exercise, the Swedish signals intelligence model and its safeguards against abuse must be seen as one whole."* (ov. 366)

    Het is goed hierbij nog op te merken dat het Hof in zijn beoordeling van het Zweedse stelsel de judiciële pre-autorisatieprocedure zoals die in Zweden bestaat als cruciaal aanmerkt*: "Crucially, the judicial pre-authorisation procedure as it exists in Sweden and the supervision exercised by an independent body in Sweden serve in principle to ensure the application of the domestic legal requirements and the Convention standards in practice and to limit the risk of disproportionate consequences affecting Article 8 rights. Notably, regard must be had to the fact that in Sweden the limits to be observed in each bulk interception mission, as well as its lawfulness and proportionality in general, are the subject matter of judicial pre-authorisation proceedings before the Foreign Intelligence Court, which sits in the presence of a privacy protection representative defending the public interest."* (ov. 368)

    De TIB-toets op de door de minister verleende toestemming voor bulkinterceptie (OOG-interceptie ex artikel 48 Wiv 2017) komt materieel overeen met de judiciële pre-autorisatie die het Hof als cruciaal aanmerkt.

    Tot slot: het eindoordeel van het Hof is uiteindelijk dat het Zweedse bulkinterceptiestelsel, bezien als geheel, niet voldoende "end-to-end"-waarborgen bevat om een adequate en effectieve garantie tegen willekeur en het risico op misbruik te bieden. Het gaat dan uiteindelijk om drie zaken: afwezigheid van een heldere regeling inzake vernietiging van geïntercepteerd materiaal dat geen persoonsgegevens bevat, de afwezigheid van een eis om bij de verstrekking van gegevens aan een buitenlandse partner de privacybelangen van de personen wier gegevens het betreft af te wegen en de afwezigheid van een effectief *ex post facto review*. Er is dan ook sprake van schending van artikel 8 EVRM.