

No.W04.16.0097/I

's-Gravenhage, 21 september 2016

Bij Kabinetsmissive van 20 april 2016, no.2016000730, heeft Uwe Majesteit, op voordracht van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, mede namens de Minister-President, de Minister van Algemene Zaken, de Minister van Defensie en de Minister van Veiligheid en Justitie, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele andere wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..), met memorie van toelichting.

Met dit wetsvoorstel wil de regering de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) 2002 vervangen met het oog op de modernisering van de bevoegdheden van de inlichtingen- en veiligheidsdiensten en de herinrichting van het stelsel van toezicht. In de adviesaanvraag verzoekt de minister van Binnenlandse Zaken en Koninkrijksrelaties de Afdeling advisering van de Raad van State met name aandacht te besteden aan twee kwesties. De eerste vraag is of naar het oordeel van de Afdeling het wetsvoorstel voldoet aan de eisen die voortvloeien uit het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Ten tweede wordt de Afdeling verzocht om in haar advies in te gaan op het in het wetsvoorstel neergelegde stelsel van strafrechtelijke handhaving met betrekking tot de daarin voorziene medewerkings- en informatieplichten; gevraagd wordt of dat nog steeds een passend stelsel is, of dat een stelsel van bestuursrechtelijke handhaving meer in de rede ligt.

Met betrekking tot de eerste vraag komt de Afdeling allereerst tot de conclusie dat het wetsvoorstel een aanzienlijk aantal belangrijke waarborgen bevat. Daarmee wordt voldaan aan enkele essentiële vereisten die door het Europees Hof voor de Rechten van de Mens (EHRM) gesteld worden. De Afdeling acht het voorstel op het punt van de vereiste deugdelijke wettelijke basis, in het licht van de kenbaarheid en voorzienbaarheid van inbreuken, adequaat. De uitbreiding van bevoegdheden, waaronder de bevoegdheid tot ongerichte interceptie van kabelgebonden communicatie acht de Afdeling op zichzelf legitiem: de noodzaak daarvan acht zij voldoende beargumenteerd. De wet bevat voorts een stelsel van waarborgen met het oog op de beginselen van proportionaliteit en subsidiariteit, alsmede criteria met betrekking tot de opslag en vernietiging van gegevens.

Hoewel de voorgestelde regeling van het toezicht tegemoet komt aan de jurisprudentie van het EHRM, heeft de Afdeling ernstige twijfels over de daadwerkelijke effectiviteit van het voorgestelde stelsel van toezicht. Het gaat er niet uitsluitend om dat een toezichtsstelsel formeel – op papier – voldoet aan de criteria die het EHRM stelt, opdat het in 'Straatsburg' *EVRM-proof* is. Het gaat er vooral om, dat het stelsel van toezicht is toegesneden op de specifieke inrichting van het nationale systeem en daarbinnen, in samenhang gezien, daadwerkelijk effectieve bescherming biedt. Het wetsvoorstel schiet op dit punt tekort. De

AAN DE KONING

Afdeling adviseert de Toetsingscommissie inzet bevoegdheden (TIB) uit het voorstel te schrappen en het toezicht – met uitzondering van de behandeling van klachten – bij de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD) te concentreren. Om deze reden adviseert zij het voorstel op dit punt niet in zijn huidige vorm aan de Kamer te zenden.

Daarnaast is de Afdeling er met betrekking tot de proportionaliteit van met name de grootschalige gegevensverzameling (Big Data) niet van overtuigd dat het voorstel en de motivering in de memorie van toelichting op alle punten daadwerkelijk voldoen aan de vereisten die voortvloeien uit het EVRM. In het bijzonder heeft de Afdeling ernstige twijfels over de verenigbaarheid met het EVRM als het gaat om de bewaartermijn van drie jaar als bedoeld in artikel 47, vijfde lid. Zij adviseert om in het wetsvoorstel een substantieel kortere bewaartermijn op te nemen

Met betrekking tot de tweede vraag komt de Afdeling tot de conclusie dat er geen aanleiding is om van het huidige stelsel van strafrechtelijke handhaving af te zien.

Vervolgens gaat de Afdeling in op enkele andere onderwerpen, waaronder de vormgeving van de TIB (indien gehandhaafd), de regeling van het mandaat en de toelichting. Naar aanleiding van deze opmerkingen adviseert de Afdeling om (delen) van het wetsvoorstel aan te passen en de opzet van de toelichting in zijn geheel te herzien.

Inhoud

1. Inleiding
 - a. Algemeen
 - b. Aanleiding voor wetsvoorstel
 - c. Kabinetsstandpunt en wetsvoorstel
2. Verenigbaarheid met het EVRM: toetsing op enkele hoofdlijnen
 - a. Inleiding: de aard van de toetsing
 - b. Bij wet voorzien: deugdelijke wettelijke basis; kenbaarheid en voorzienbaarheid
 - c. Noodzakelijk in een democratische samenleving
 - d. Tussenconclusie
 - e. Toezicht en Big Data
3. Effectief toezicht
 - a. Straatsburgse rechtspraak: hoofdlijnen
 - b. Artikel 13 EVRM: 'effectief' toezicht
 - c. Effectiviteit van de toetsing door de TIB
 - d. Effectiviteit van het toezicht door de CTIVD
 - e. Klachtrecht
 - f. Conclusie
4. Gegevensverwerking: Big Data
 - a. Het belang en de risico's van Big Data
 - b. Een samenhangende visie
 - c. Transparantie werkwijze
 - d. Driefasenaanpak en toestemming
 - e. Uitwerking onderzoeksoopdrachtgerichte interceptie
 - f. Vernietiging niet onderzochte gegevens
 - g. Vernietiging niet relevante gegevens
 - h. Vernietiging versleutelde gegevens
 - i. Samenwerking buitenland
 - j. Profileren en geautomatiseerde besluitvorming
 - k. Aanpassing technische systemen
5. Slotconclusie: verenigbaarheid met het EVRM
6. Strafrechtelijke handhaving medewerkingsplicht
7. Vormgeving TIB
 - a. Enkelvoudige of meervoudige samenstelling
 - b. Benodigde deskundigheid
 - c. Verantwoording
 - d. conclusie
8. Mandaat
9. Binnendringen van een geautomatiseerd werk van een derde
10. Toelichting
11. Overige opmerkingen
 - a. Samenhang met het wetsvoorstel bronbescherming in strafzaken
 - b. Medewerkingsplicht oud-medewerkers
 - c. "Mededeling" of "verstrekking"
12. Conclusie en dictum

1. Inleiding

a. *Algemeen*

De toelichting op het wetsvoorstel stelt terecht dat “een belangrijke kerntaak van de overheid is het garanderen van een veilig land waarin in vrijheid kan worden geleefd en de democratische rechtsorde is gewaarborgd”.¹ De Afdeling is met de regering van oordeel dat inlichtingen- en veiligheidsdiensten noodzakelijk zijn om deze kerntaak van de overheid te vervullen, omdat de democratische rechtsorde slechts bij de gratie van veiligheid kan functioneren. De diensten verrichten met het oog hierop onderzoek naar organisaties en personen die (vermoedelijk) een gevaar vormen voor de nationale en/of internationale veiligheid. Aldus beschermen de diensten de democratische rechtsstaat en dragen zij bij aan het waarborgen van de grondrechten van haar burgers.² In die zin zijn de diensten essentieel – opdat burgers in onze samenleving in vrijheid en veiligheid kunnen leven.

Om effectief te kunnen zijn in het identificeren van gevaarlijke organisaties en personen dient het onderzoek van de diensten in het algemeen heimelijk te kunnen geschieden, zonder dat de betrokkenen hiervan weet hebben. De omvang van deze heimelijk uitgeoefende bevoegdheden moet corresponderen met de reële risico's waarmee de Nederlandse samenleving en de daarmee verbonden internationale rechtsorde thans worden geconfronteerd. Die risico's zijn de afgelopen jaren sterk toegenomen. In het bijzonder kan gewezen worden op de terroristische dreigingen en cybercrime-gevaren, alsmede op de veiligheidsrisico's die samenhangen met de brandhaarden aan de randen van Europa.³ Bepalend voor de omvang van die risico's zijn ook de hieraan gerelateerde technologische ontwikkelingen,⁴ die digitale aanvallen van vitale ict-infrastructuren – niet alleen van het bedrijfsleven, maar ook van de overheid en zelfs van de inlichtingen- en veiligheidsdiensten zelf – mogelijk maken.⁵

Tegelijkertijd stellen deze technologische ontwikkelingen de diensten in staat om zelf met het oog op voorkoming van de geschetste dreigingen en aanvallen grote hoeveelheden data omtrent mogelijk gevaarlijke personen en groepen te verzamelen en te analyseren. Deze ontwikkelingen brengen met zich, dat de diensten meer dan voorheen en in toenemende mate niet alleen reactief, gebaseerd op een geconstateerde actuele dreiging, maar ook pro-actief, met het

¹ Aldus de toelichting, paragraaf 1.1.

² Zie ook de evaluatie door de Commissie Dessens van de Wet op de inlichtingen- en veiligheidsdiensten 2002, *Naar een nieuwe balans tussen bevoegdheden en waarborgen* (hierna: Dessens 2013), blz. 78-79 en Venice Commission, *Report on the Democratic Oversight of the Security Services*, CDL-AD(2015)010 (hierna: Venice Commission 2015a), par. 54-55.

³ Zie in deze zin de toelichting, paragrafen 1.1 en 1.3.

⁴ Aldus Kamerstukken II 2015/16, 26 643, nr. 420 en het bijbehorende *Cybersecuritybeeld Nederland 2016 (CSBN 2016)*.

⁵ Toelichting, paragraaf 1.3. Vgl. Venice Commission 2015a, par. 58-59: ‘Globalization and the complexity of modern societies increases their vulnerability to national and transnational terrorism. Industrial and technologically based economies require a relatively high level of order and stability and a small group of determined people can do a vast amount of damage to the communications, transport or power networks.’

oog het in kaart brengen van mogelijke dreigingen, kunnen en ook moeten opereren.

Gezien de toenemende bedreigingen van de nationale veiligheid en individuele vrijheid wordt voorgesteld de bijzondere bevoegdheden van de diensten, die diep in de persoonlijke levenssfeer kunnen ingrijpen, verder uit te breiden. Deze noodzakelijke uitbreiding van ingrijpende bevoegdheden vergroot tegelijkertijd het spanningsveld, waarbij de diensten enerzijds ten dienste van het waarborgen van de rechtsstaat en de daarin beschermde grondrechten optreden, maar daarbij tevens vergaande inbreuken op die grondrechten kunnen maken. De toelichting wijst terecht op deze inherente spanning.⁶ Ook de Commissie Dessens, die de Wiv 2002 evalueerde, stelde eerder reeds dat een balans moet worden gevonden tussen enerzijds de effectiviteit van het operationele vermogen van de diensten (omvang van de bijzondere bevoegdheden; geheimhouding; capaciteit) en anderzijds het waarborgen van grondrechten inclusief daarop gericht effectief toezicht op het werk van de diensten.⁷

De Afdeling onderschrijft zoals gezegd het cruciale belang van goed functionerende inlichtingen- en veiligheidsdiensten ten behoeve van de bescherming van de democratische rechtsstaat. Het is met het oog daarop noodzakelijk dat de diensten gezien hun taak – mede gericht op het beschermen van de vrijheid en veiligheid van burgers – over voldoende effectieve bevoegdheden en middelen beschikken. In dat licht bezien acht de Afdeling de voorgestelde uitbreiding van bevoegdheden legitiem en noodzakelijk. Met uitbreiding van bevoegdheden kan evenwel niet worden volstaan. Om het noodzakelijke vertrouwen van burger en samenleving in de inlichtingen- en veiligheidsdiensten te waarborgen dient de wetgever te voorkomen dat de diensten op disproportionele wijze ingrijpen in de persoonlijke levenssfeer van burgers en dient hij, om dat doel te bereiken, in de wet waarborgen te formuleren waarbinnen de diensten moeten opereren. Met het oog daarop moet er in het bijzonder een effectief stelsel van toezicht worden ingericht, juist omdat het optreden van de diensten in het algemeen een geheim karakter heeft. Tegelijkertijd moet daardoor de slagkracht van de diensten – wier functioneren uiteindelijk evenzeer gericht is op grondrechtenbescherming – niet in gevaar komen.

De Afdeling erkent de complexiteit van de opdracht om een balans te vinden tussen enerzijds de vereiste effectiviteit van de diensten, die onmisbaar is omwille van de handhaving van de democratische rechtsstaat, en anderzijds de noodzaak van een effectieve begrenzing van het opereren van die diensten, met het oog op het voorkomen van te vergaande beperkingen op de door de democratische rechtsstaat verzekerde grondrechten van burgers. De Afdeling maakt haar opmerkingen bij het voorgelegde wetsvoorstel dan ook met het oog op de ook door de regering nagestreefde balans.⁸

⁶ Toelichting, paragraaf 1.1.

⁷ Dessens 2013, blz. 8.

⁸ Toelichting, paragraaf 1.2.

b. *Aanleiding voor wetsvoorstel*

De regering stelt in de toelichting dat de bestaande wet, de Wiv 2002, toe is aan een grondige herziening. Gewezen wordt op technologische, maatschappelijke en juridische ontwikkelingen die noodzaken tot modernisering van de bevoegdheden van de inlichtingen- en veiligheidsdiensten.⁹ Nieuwe vormen van communicatie zijn dominant geworden: zo heeft er een fundamentele verschuiving plaatsgevonden van communicatie via ether en satelliet naar communicatie via kabelnetwerken. Ook juridische ontwikkelingen zijn relevant voor de noodzaak de Wiv te moderniseren. Mede onder invloed van de jurisprudentie van het EHRM¹⁰ is de aandacht voor de democratisch-rechtsstatelijke inbedding van de diensten en het toezicht daarop sterk toegenomen.

Tegen de hierboven geschetste achtergrond heeft de Commissie Dessens in het kader van haar evaluatie van de Wiv 2002 aanbevelingen gedaan tot fundamentele aanpassing van de huidige wet. De belangrijkste wijzigingen waartoe zij adviseert betreffen de inzet van de bijzondere bevoegdheden en het toezicht daarop. De Commissie wijst erop dat de interceptiebevoegdheden in de Wiv 2002 techniekafhankelijk zijn geformuleerd. Het daarin gemaakte onderscheid tussen communicatie via 'de ether' (waarbij ongerichte 'bulk' interceptie toelaatbaar is) en 'de kabel' (waarbij ongerichte interceptie niet toegestaan is) rijmt niet meer met de snel voortschrijdende technologische ontwikkelingen op het gebied van dataverkeer en communicatie. Dit onderscheid zou daarom moeten worden opgeheven. Tegelijkertijd zou een herziening en versteviging van de wettelijke waarborgen met betrekking tot de ministeriële toestemming en het toezicht door de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD) plaats dienen te vinden. Deze waarborgen zouden gekoppeld moeten worden aan de uitoefening van de bijzondere interceptiebevoegdheden.¹¹

c. *Kabinetsstandpunt en wetsvoorstel*

De regering heeft in het voorliggende wetsvoorstel veel van de aanbevelingen van de Commissie Dessens overgenomen. De meest in het oog springende wijziging betreft het mogelijk maken van (bulk)interceptie van kabelgebonden telecommunicatie. Daaraan gekoppeld zou toezicht op de uitoefening van deze ingrijpende bijzondere bevoegdheden door de CTIVD uitgeoefend moeten worden. Anders dan de Commissie Dessens was de regering er echter geen voorstander van om de rechtmatigheidsoordelen van de CTIVD een juridisch bindende kracht te geven, en stelde stelde zij in het consultatiewetsvoorstel een 'heroverwegingsstelsel' voor. Dat hield in, dat indien de CTIVD in het kader van haar rechtmatigheidstoezicht tot de conclusie kwam dat een verleende toestemming onrechtmatig was, de minister verplicht zou zijn deze te

⁹ De regering sluit op dit punt grotendeels aan bij de conclusies en aanbeveling van de Commissie Dessens, Evaluatie Wet op de veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen, 2013.

¹⁰ Bij wijze van voorbeeld wijst de Afdeling op de discussie omtrent de bevoegdheden van diensten gericht op het achterhalen van de bron van een journalist. De regeling in het voorgestelde artikel 29, vijfde lid, vloeit voort uit het arrest van het EHRM van 22 november 2012, 39315/06, Telegraaf Media Nederland Landelijke Media B.V. e.a. t. Nederland.

¹¹ Commissie Dessens, hoofdstuk 5.

heroverwegen. Indien de minister na heroverweging persisteerde in de verleende toestemming dienden de beide Kamers van de Staten-Generaal hiervan, al dan niet in vertrouwelijke vorm,¹² onverwijld op de hoogte te worden gesteld. In concreto betekent dit meestal, dat het vanwege de noodzakelijke vertrouwelijkheid aan de parlementaire commissie inzake de Inlichtingen- en veiligheidsdiensten (CVID) zou zijn om de minister ter verantwoording te roepen.¹³

In de consultatiefase met betrekking tot het conceptwetsvoorstel zijn veel kritische opmerkingen gemaakt over de uitbreiding van de interceptiebevoegdheden en het bijbehorende stelsel van toezicht. Naar aanleiding daarvan heeft de regering er voor gekozen in het voorliggende wetsvoorstel het 'heroverwegingsstelsel' met betrekking tot de inzet van bijzondere bevoegdheden te vervangen door een *bindende* rechtmatigheidstoetsing van de ministeriële toestemming. Deze bindende toetsing zal worden uitgevoerd door een nieuw in te stellen Toetsingscommissie inzet bevoegdheden, de TIB.¹⁴ De TIB bestaat uit één lid en ten minste twee plaatsvervangende leden, die benoemd worden door de regering op voordracht van de betrokken ministers. Daarbij putten de ministers uit een voordracht van de Tweede Kamer van ten minste drie personen per vacature. Leden van de TIB hebben tenminste zes jaar rechterlijke ervaring. Zij worden voor zes jaar benoemd, met een mogelijkheid van een eenmalige herbenoeming.

2. Verenigbaarheid met het EVRM: toetsing op enkele hoofdlijnen

a. *Inleiding: de aard van de toetsing*

Vooraf merkt de Afdeling op dat de vraag of het wetsvoorstel voldoet aan de eisen die voortvloeien uit het EVRM niet eenvoudig en niet met zekerheid beantwoord kan worden. De uitspraken van het EHRM zien primair op de aan het Hof voorgelegde concrete casus en op de omstandigheden alsmede de wetgeving en praktijk in de betreffende verdragsstaat. De wetgeving en praktijk van de betreffende verdragsstaten verschilt veelal fundamenteel van het Nederlandse systeem.¹⁵ Uitspraken met betrekking tot andere stelsels hebben in het algemeen uitsluitend betrekking hebben op het concrete geval. Gezien het – op de voorgelegde casus en de toepasselijke wetgeving en praktijk – toegespitste karakter van de Hof-jurisprudentie zijn deze uitspraken dan ook niet één op één te transponeren naar de Nederlandse situatie.

Het stelsel zoals in de WIV 2002 is neergelegd is tot op heden nog niet ten gronde door het EHRM beoordeeld. Wel heeft het Hof ten aanzien van stelsels van andere verdragsstaten enkele uitspraken gedaan waarin algemene uitgangspunten zijn geformuleerd, die de Afdeling bij haar beoordeling zal betrekken. Een van deze

¹² Artikel 102, derde lid jo. artikel 12, vierde lid van het consultatievoorstel.

¹³ Toelichting bij het consultatiewetsvoorstel, paragraaf 7.3.2.

¹⁴ Artikelen 31 en 32 van het voorstel.

¹⁵ Zie voor een overzicht van de verschillende systemen van toezicht op de veiligheidsdiensten in de EU-lidstaten: European Union Agency for Fundamental Rights (FRA), *Surveillance by intelligence services; fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks*, 2015. Hoofdstuk 10 van de toelichting biedt een handzaam overzicht van de in Duitsland, Verenigd Koninkrijk, Frankrijk en België vigerende toezichtsstelsels.

algemene uitgangspunten is dat het EHRM bij zijn beoordeling steeds onderstreept dat het gaat om het *gehele systeem* van (nationale) waarborgen en de effectiviteit van die waarborgen in hun onderlinge samenhang.¹⁶ Dit betekent dat eventuele beperkingen ten aanzien van een bepaald aspect veelal kunnen worden gecompenseerd door andere waarborgen.¹⁷

Tegen deze achtergrond gaat de Afdeling eerst over tot een beoordeling op enkele hoofdlijnen wat betreft de verenigbaarheid van het wetsvoorstel met de vereisten die voortvloeien uit het EVRM. Daarbij gaat zij in het bijzonder in op de eisen die voortvloeien uit artikel 8, tweede lid, EVRM, te weten het legaliteitsbeginsel (onderdeel b) en de vereisten van noodzakelijkheid en proportionaliteit (onderdeel c). Vervolgens gaat de Afdeling specifiek in op de effectiviteit van het voorgestelde toezichtstelsel (punt 3) en op de proportionaliteit van de bevoegdheden tot verwerving en verwerking van Big Data (punt 4). In punt 5 wordt een en ander afgerond met een concluderende beschouwing.

b. *Bij wet voorzien: deugdelijke wettelijke basis; kenbaarheid en voorzienbaarheid*

Het optreden van inlichtingen- en veiligheidsdiensten zal in het algemeen gepaard gaan met inbreuken op het EVRM, in het bijzonder op het recht op bescherming van de persoonlijke levenssfeer.¹⁸ Bij het maken van zo een inbreuk op grondrechten door de inlichtingen- en veiligheidsdiensten vloeit uit het EVRM voort dat deze bij wet moet zijn voorzien. Dat vereist dat er een basis voor de inbreuk is in nationale regelgeving, welke toegankelijk is en waarvan de effecten voldoende voorzienbaar zijn.¹⁹ Aan de eerste twee voorwaarden – de wettelijke basis en de toegankelijkheid – is in ieder geval met de voorgestelde regeling voldaan.

De vraag rijst of ook voldaan wordt aan het *voorzienbaarheidsvereiste*. Dit vereiste gaat met betrekking tot geheime surveillancemaatregelen van inlichtingen- en veiligheidsdiensten niet zo ver dat een individu in staat moet zijn te voorzien wanneer deze diensten zijn communicatie onderscheppen en daarop zijn gedrag aan te passen. Wel moet de wet de reikwijdte van de bevoegdheden van de diensten en de toepassing daarvan met voldoende helderheid aangeven, om het

¹⁶ EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 72; cf. EHRM 26 oktober 2000, 30210/96, Kudla t. Polen, par. 157; EHRM 13 december 2012, 22689/07, De Souza Ribeiro t. Frankrijk, par. 79.

¹⁷ EHRM 26 maart 1987, nr. 9248/81, Leander t. Zweden; EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland; EHRM 18 mei 2010, 26839/05, Kennedy t. Verenigd Koninkrijk). Zie ook Venice Commission 2015a, par. 111-112.

¹⁸ Artikel 8 EVRM.

¹⁹ EHRM 22 november 2012, 39315/06, Telegraaf Media Nederland Landelijke Media B.V. e.a. t. Nederland, par. 90: 'the expression 'in accordance with the law' not only requires the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects.' In dezelfde zin EHRM 24 april 1990, 11801/85, Kruslin t. Frankrijk, par. 30 e.v., EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 84; EHRM 6 juni 2006, 62332/00, Segerstedt-Wiberg en anderen t. Zweden, par. 76.

individuele adequate bescherming te bieden tegen arbitraire inbreuken op zijn persoonlijke levenssfeer.²⁰

In de ontvankelijkheidsbeslissing in *Weber en Saravia* heeft het Hof een en ander nader gepreciseerd. Zo dient de aard van de strafbare overtredingen die tot inzet van een interceptiebevoegdheid kunnen leiden alsmede de categorieën van personen wier telefoon getapt kan worden in de wet omschreven te worden.²¹ In lijn hiermee oordeelde het Hof in *Liberty* onder meer dat vanwege het hanteren van abstracte termen zoals 'nationale veiligheid' ter rechtvaardiging van grootschalige interceptie van communicatie met het buitenland sprake was van een ongerechtvaardigde inbreuk op artikel 8 EVRM.²²

Uit deze jurisprudentie vloeit evenwel niet voort dat de wettelijke regeling van de bevoegdheden van de diensten een opsomming zou moeten bevatten van de (dreigende) misdrijven die grond zouden kunnen vormen voor het inzetten van hun interceptiebevoegdheden. De Wiv 2002 en het wetsvoorstel²³ zien immers uitsluitend op het doel van de nationale veiligheid, los van strafrechtelijke connotaties.²⁴ Daarnaast wijst de Afdeling er op dat het Hof in *Kennedy* oordeelde dat het hanteren van het criterium als 'nationale veiligheid' met het oog op interceptie geen strijd hoeft op te leveren met het legaliteitsvereiste.²⁵ In de *Telegraaf*-zaak ten slotte oordeelde het Hof dat het op grond van artikel 6, tweede lid, onder a van de WIV 2002²⁶ af luisteren van advocaten met het oog op het achterhalen van hun bronnen in het licht van artikel 8, tweede lid, van het EVRM een voldoende voorzienbare, wettelijke grondslag vormde.²⁷

Daarnaast is van belang dat het wetsvoorstel de bevoegdheden van de diensten niet alleen bindt aan het belang van de nationale veiligheid, maar deze ook nader toespitst op specifieke taken.²⁸ Zoals de toelichting uiteenzet²⁹ mogen slechts ter uitvoering van een deel van deze taken³⁰ bijzondere bevoegdheden die ingrijpende

²⁰ EHRM 26 maart 1987, 9248/81, *Leander t. Zweden*, par. 51.

²¹ EHRM 29 juni 2006, 54934/00, *Weber en Saravia t. Duitsland*, par. 95: 'In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; [...].

²² EHRM 1 juli 2008, 58243/00, *Liberty t. Verenigd Koninkrijk*, par. 64-69.

²³ De artikelen 8, tweede lid, en 10, tweede lid, van het voorstel.

²⁴ Vergelijk artikel 13 van het voorstel.

²⁵ EHRM 18 mei 2010, 26839/05, *Kennedy t. Verenigd Koninkrijk*, par. 159.

²⁶ De AIVD heeft 'in het belang van de nationale veiligheid' tot taak 'het verrichten van onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat'.

²⁷ EHRM 22 november 2012, 39315/06, *Telegraaf Media Nederland Landelijke Media B.V. e.a. t. Nederland*, par. 90-93.

²⁸ De artikelen 8, tweede lid, en 10, tweede lid, van het voorstel.

²⁹ Toelichting, paragraaf 9.2.1.

³⁰ De artikelen 8, tweede lid, onder a en d en 10, tweede lid, onder a, c en e van het voorstel.

inbreuken op de persoonlijke levenssfeer maken, ingezet worden.³¹ Deze inzet is omgeven met sterke waarborgen, waarop hierna nader zal worden ingegaan (zie punt c). Ten behoeve van de overige taken kunnen uitsluitend de in artikel 25, eerste lid neergelegde, minder ingrijpende bevoegdheden worden ingezet.

c. *Noodzakelijk in een democratische samenleving*

Een beperking of inbreuk op grondrechten, zoals artikel 8 EVRM is alleen toegestaan indien sprake is van een legitiem doel, een dwingende maatschappelijke noodzaak voor de inbreuk ("*pressing social need*") en de inbreuk ook proportioneel is aan het na te streven doel. De lidstaten hebben hierbij een eigen beoordelingsruimte ("*margin of appreciation*"), maar het EVRM houdt hierop wel toezicht.³²

Zoals de Afdeling hiervoor heeft opgemerkt en zoals blijkt uit de jurisprudentie van het EHRM, staat buiten twijfel dat goed functionerende inlichtingen- en veiligheidsdiensten en de middelen die zij inzetten noodzakelijk zijn om het legitieme doel van bescherming van de nationale veiligheid na te streven.³³ Er is gezien de technologische ontwikkelingen, waarin de kabelgebonden telecommunicatie in verhouding tot de niet-kabelgebonden telecommunicatie explosief is gegroeid, alsmede gelet op de bedreigingen waarmee de Nederlandse samenleving geconfronteerd wordt, voldoende grond om aan te nemen dat de in het wetsvoorstel opgenomen bevoegdheden tot interceptie van bulk-communicatie (artikelen 47-49) met het oog op dat doel op zichzelf noodzakelijk geacht kunnen worden. De Afdeling is het met de regering³⁴ eens dat het huidige onderscheid in de Wiv 2002 tussen communicatie via de 'ether' (ten aanzien waarvan ongerichte 'bulk' interceptie reeds toegelaten is) en de 'kabel' (ten aanzien waarvan alleen gerichte interceptie toegelaten is) niet gehandhaafd kan worden, en dat mede gelet daarop de genoemde uitbreiding van de bevoegdheden ten aanzien van kabelgebonden communicatie in het licht van het EVRM gerechtvaardigd is.³⁵

Wel moet worden gezien of wordt voldaan aan de vereisten van *subsidiariteit en proportionaliteit*. Het EHRM beoordeelt dit steeds op basis van de omstandigheden van het geval. Daarbij gaat het om het type bevoegdheid dat wordt ingezet; de ingrijpendheid van die bevoegdheid en de duur waarvoor deze kan worden ingezet; de motieven voor de inzet; het stelsel van goedkeuring van de inzet van de bevoegdheid en het toezicht hierop; en de rechtsmiddelen die de burger ter

³¹ Artikel 28, eerste lid, van het voorstel, met een beperkte uitzondering in het tweede lid.

³² Zie bijvoorbeeld EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 49.

³³ EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 78-79; EHRM 1 juli 2008, 58243/00, Liberty e.a. t. Verenigd Koninkrijk par. 58; EHRM 18 mei 2010, 26839/05, Kennedy t. Verenigd Koninkrijk, par. 155; EHRM 2 september 2010, 35623/05, Uzun t. Duitsland ro. 77; EHRM 18 april 2013, 19522/09, M.K./Frankrijk par. 29.

³⁴ Toelichting, paragrafen 1.3-1.6, 3.3.4.4.7.4 en 12.2.2, in het voetspoor van Dessens 2013, hoofdstuk 5 en par. 8.5.

³⁵ In EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland en EHRM 1 juli 2008, 58243/00, Liberty t. Verenigd Koninkrijk maakte het Hof dit onderscheid dan ook niet.

beschikking staan tegen de inzet van bevoegdheden.³⁶ Met betrekking tot de inzet van ongerichte interceptie lijkt het Hof de nadruk vooral te leggen op de procedurele inbedding van de bevoegdheden en met name de manier waarop een bevel tot inzet tot stand komt, de controle op de uitvoering hiervan en de aanwezigheid van onafhankelijk toezicht.³⁷

In het licht van de vereisten van proportionaliteit en subsidiariteit acht het EHRM de inzet van heimelijke interceptiebevoegdheden op zichzelf toelaatbaar. Wel moet steeds de evenredigheid van het belang van het onderzoek worden afgewogen tegenover de inbreuk die hiermee gemaakt wordt op de grondrechten van burgers.³⁸ Daarbij moet ook worden gezien of niet volstaan kan worden met een bevoegdheid die minder ingrijpend is. Met het oog daarop is van belang dat de vereisten van proportionaliteit en subsidiariteit in de artikelen 18 en 26 van het wetsvoorstel geformuleerd zijn als algemene uitgangspunten die bij de uitoefening van bevoegdheden tot het verzamelen en verwerken van gegevens in acht moeten worden genomen. Dat is terecht, nu het verwerven en verwerken van gegevens de kern van het werk van de diensten vormt. De Afdeling gaat er van uit dat deze algemene beginselen betrekking hebben op alle bevoegdheden van de diensten³⁹, en steeds gelezen moeten worden in samenhang met het primaire doel van de diensten, het belang van de nationale veiligheid (artikelen 8, eerste lid, en 10, eerste lid).

Daarnaast ligt in artikel 28, eerste lid – met een beperkte uitzondering in het tweede lid – het noodzakelijkheidsvereiste besloten met betrekking tot de inzet van de (meest) ingrijpende bijzondere bevoegdheden als bedoeld in paragraaf 3.2.5 van het voorstel. Artikel 29, eerste en tweede lid, geeft een bevoegdheidsregeling, terwijl het derde lid grenzen stelt met betrekking tot de duur van de inzet van de betreffende bevoegdheden. Deze bevoegdheden vinden een specifieke regulering in de artikelen 39-57, en kunnen slechts uitgeoefend worden na toestemming door de TIB.⁴⁰ Op de uitvoering van deze en andere bevoegdheden houdt de CTIVD toezicht.⁴¹

Verder bevat het voorstel waarborgen met betrekking tot de opslag, lengte van de bewaartermijnen en vernietiging van gegevens, die medebepalend zijn voor de verstrekking van de inbreuk op de persoonlijke levenssfeer. Artikel 27 geeft een algemene regeling van termijnen en vernietigingsplichten; de artikelen 46-48 bevatten enkele meer specifieke regelingen.⁴² Ten slotte bevat het voorstel een

³⁶ EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 50 en EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 106.

³⁷ EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 115-117. Zie ook EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 232.

³⁸ EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland.

³⁹ Bijvoorbeeld de bevoegdheid van toegang tot plaatsen als bedoeld in artikel 57.

⁴⁰ Ingevolge de artikelen 35 en 36 van het voorstel.

⁴¹ Artikel 95, derde lid, van het voorstel.

⁴² Zie punt 4 voor kritische kanttekeningen bij die specifieke regelingen

plicht tot notificatie⁴³ met betrekking tot het openen van brieven en andere zendingen⁴⁴, het 'gericht tappen'⁴⁵ en het binnentreden in de zin van artikel 57.

d. *Tussenconclusie*

Het wetsvoorstel bevat een aanzienlijk aantal belangrijke waarborgen. Daarmee wordt voldaan aan enkele essentiële vereisten die door het EHRM gesteld worden. De Afdeling acht het voorstel op het punt van de vereiste deugdelijke wettelijke basis, in het licht van de kenbaarheid en voorzienbaarheid van inbreuken, adequaat. De uitbreiding van bevoegdheden, waaronder de bevoegdheid tot ongerichte interceptie van kabelgebonden communicatie acht de Afdeling op zichzelf legitiem: de noodzaak daarvan acht zij voldoende beargumenteerd. De wet bevat voorts een stelsel van waarborgen met het oog op de beginselen van proportionaliteit en subsidiariteit, alsmede criteria met betrekking tot de opslag en vernietiging van gegevens.

e. *Toezicht en Big Data*

De Afdeling heeft echter – zoals hierna zal blijken – ernstige twijfels over de *daadwerkelijke effectiviteit* van het voorgestelde stelsel van toezicht. Benadrukt moet worden dat de verplichting op grond van het EVRM om te voorzien in een effectief stelsel van toezicht primair op de verdragsstaat rust, niet op het – van een afstand oordelende – Hof in Straatsburg. Het gaat er dan ook niet enkel om dat een toezichtstelsel formeel – op papier – voldoet aan de criteria die het EHRM stelt, opdat het in 'Straatsburg' aanvaardbaar is.⁴⁶ Het gaat er vooral om, dat het stelsel van toezicht is toegesneden op de specifieke inrichting van het nationale systeem, en daarbinnen daadwerkelijk effectieve bescherming biedt. Als daaraan voldaan is, zal dat stelsel ook *EVRM-proof* zijn.

Daarnaast is de Afdeling er met betrekking tot de proportionaliteit van met name grootschalige gegevensverzameling (Big Data) voorshands niet van overtuigd dat het voorstel en de motivering in de memorie van toelichting op alle punten daadwerkelijk voldoen aan de vereisten die voortvloeien uit het EVRM. In het bijzonder heeft de Afdeling ernstige twijfels over de verenigbaarheid met het EVRM als het gaat om de bewaartermijn van drie jaar als bedoeld in artikel 47, vijfde lid.

Deze twee punten – het toezicht en Big Data – verdienen afzonderlijke bespreking in respectievelijk punt 3 en 4. In punt 5 volgt met betrekking tot de verenigbaarheid met het EVRM de eindconclusie.

⁴³ Artikel 58 van het voorstel.

⁴⁴ Artikel 43 van het voorstel.

⁴⁵ Artikel 46 van het voorstel.

⁴⁶ Vgl. de toelichting, paragraaf 12.2.3, waaruit blijkt dat de introductie van de TIB met name ingegeven is om te bewerkstelligen dat het toezichtsstelsel *EVRM-proof* is.

3. Effectief toezicht

a. *Straatsburgse rechtspraak: hoofdlijnen*

Het EHRM benadrukt steeds het belang van adequaat *toezicht* op de inzet en uitoefening van de bevoegdheden van inlichtingen- en veiligheidsdiensten, een vereiste dat voortvloeit uit artikel 13 EVRM. Een adequate invulling van het toezicht op de werkzaamheden van de inlichtingendiensten moet compensatie bieden voor het feit dat degenen die onderzocht worden hiervan veelal geen weet zullen hebben. Dit betekent dat betrokkenen vaak zelf geen mogelijkheden hebben om een beroep te doen op de rechter of andere instanties indien zij menen dat er ten onrechte een inbreuk wordt gemaakt op hun rechten. Om die reden is van belang dat een onafhankelijke instantie controleert of de diensten opereren binnen hun bevoegdheden, op grond van de juiste procedures en met inachtneming van eisen van proportionaliteit en subsidiariteit. Dit toezicht dient zich uit te strekken tot de verschillende fasen van het onderzoek, moet onafhankelijk en – zoals artikel 13 EVRM uitdrukkelijk stelt – effectief zijn.⁴⁷

Bij de vormgeving van het toezichtstelsel is onder meer de democratische inbedding van het functioneren van de inlichtingen- en veiligheidsdiensten van belang. Het EHRM houdt bij de eisen die het stelt aan het externe toezicht immers rekening met de wijze waarop de interne procedures van toestemming voor de uitoefening van bevoegdheden zijn vormgegeven.⁴⁸ Dit betekent dat een goed functionerend toezicht vanuit het parlement op de wijze waarop de minister de diensten aanstuurt bij de beoordeling of het stelsel van toezicht effectief is meegewogen dient te worden.

Het systeem van ministeriële toestemming en de aan de ministeriële verantwoordelijkheid gekoppelde parlementaire controle vormen belangrijke elementen in de Wiv 2002. Daarin is er bewust voor gekozen om het onafhankelijk toezicht door de CTIVD niet vooraf te laten plaatsvinden, omdat “de besluitvorming over de wijze waarop deze diensten hun taken uitvoeren (al dan niet in mandaat) dient plaats te vinden onder de volledige verantwoordelijkheid van de desbetreffende minister die daarover achteraf verantwoording aflegt aan de daarvoor in aanmerking komende instanties (parlement, rechter, commissie van toezicht).”⁴⁹

Het belang van een goed functionerende ministeriële verantwoordelijkheid en parlementaire controle betekent evenwel niet dat rechtmatigheidscontrole door een onafhankelijke toezichthouder niet nodig is.⁵⁰ De introductie in het wetsvoorstel van de TIB beoogt tegemoet te komen aan de kritiek die in de consultatiefase is

⁴⁷ Zie bijvoorbeeld EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 249, 267, 285.

⁴⁸ EHRM 29 juni 2006, no. 54934/00, Weber en Saravia t. Duitsland, par. 32 en 117; EHRM 18 mei 2010, 26839/05, Kennedy t. Verenigd Koninkrijk, par. 61 en 166.

⁴⁹ Kamerstukken II 1999/2000, 25 877, nr. 8, blz. 108.

⁵⁰ Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten, Universiteit Leiden, blz. 13. Dit rapport is een bijlage bij de reactie van de CTIVD op de consultatieversie van het wetsvoorstel.

geuit op het ontbreken van een voorafgaande onafhankelijke toetsing van de inzet van bijzondere bevoegdheden door de diensten.⁵¹ In verschillende reacties werd gesteld dat zonder een dergelijke voorafgaande toets niet zou worden voldaan aan de vereisten die het EHRM stelt.⁵²

De regering stelt in de toelichting dat uit de jurisprudentie van het EHRM een voorkeur voor een dergelijke toets spreekt. Zij verwijst voor die conclusie naar het rapport 'Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten' van de Universiteit Leiden. Of voorafgaande onafhankelijke toetsing dwingend voortvloeit uit de vereisten die het EHRM stelt, laat zij echter in het midden. Daarnaast wordt de introductie van de TIB blijkens de toelichting ingegeven door de wens om daarmee tegemoet te komen aan maatschappelijke zorgen over de inbreuk op de persoonlijke levenssfeer die gepaard kan gaan met de mogelijkheid tot kabelgebonden interceptie.⁵³

De jurisprudentie van het EHRM inzake het vereiste van onafhankelijke toetsing op de inzet van bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten is evenwel niet eenduidig. Weliswaar acht het EHRM voorafgaande *rechterlijke* controle op de inzet van de bevoegdheden van de diensten wenselijk⁵⁴, maar sluit het andere vormen van toezicht, mits onafhankelijk en effectief, niet uit.⁵⁵ Alleen voor zover het de inzet van bevoegdheden jegens journalisten en advocaten betreft, is duidelijk dat een voorafgaande bindende toets door een rechterlijke instantie vereist wordt.⁵⁶ Het wetsvoorstel bevat op dit punt daarom een regeling waarin is voorzien in het vereiste van rechterlijke goedkeuring (artikel 27, tweede lid en artikel 29, vijfde en zesde lid).

Buiten die specifieke gevallen laat het Hof de lidstaten echter aanzienlijk meer ruimte, zoals blijkt uit het arrest *Kennedy*. Het Britse systeem van toezicht, waarin toestemming wordt gegeven door de minister, werd, in samenhang met onafhankelijk toezicht tijdens en na afloop van de bevoegdheidsuitoefening en een bindende klachtenprocedure, door het EHRM als voldoende gekwalificeerd.⁵⁷ De strengere lijn waar het journalisten en advocaten betreft die het EHRM volgt in andere arresten, kan mede verklaard worden doordat daarbij steeds ook andere grondrechten dan het grondrecht op bescherming van de persoonlijke levenssfeer

⁵¹ Zoals hiervoor vermeldt, oordeelt de TIB niet over de inzet van bevoegdheden jegens advocaten en journalisten. In dat geval is voorzien in een voorafgaande rechterlijke toets.

⁵² Zie onder meer de reacties van de Nationale ombudsman, het College voor de Rechten van de Mens, NJCM, Privacy First en Bits of Freedom.

⁵³ Toelichting, paragraaf 3.3.3.1.

⁵⁴ EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 34-36; EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 32; EHRM 18 mei 2010, 26839/05, Kennedy t. Verenigd Koninkrijk, par. 167; en meer recent EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 233.

⁵⁵ EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland en EHRM 18 mei 2010, 26839/05, Kennedy t. Verenigd Koninkrijk. Zie ook EHRM 8 maart 2011, 12739/05 Goranova-Karaeneva t. Bulgarije par. 49-50.

⁵⁶ Met betrekking tot journalisten: EHRM 22 november 2012, 39315/06, Telegraaf Media Nederland Landelijke Media B.V. e.a. t. Nederland

⁵⁷ EHRM 18 mei 2010, 26839/05, Kennedy t. Verenigd Koninkrijk, par. 166-169 en 196.

in het geding zijn. Het af luisteren of tappen van journalisten kan een inbreuk vormen op de in artikel 10 EVRM vervatte vrijheid van meningsuiting en de belangrijke rol van de pers daarbij. Bij advocaten is het recht op een eerlijk proces als bedoeld in artikel 6 EVRM in het geding. Bovendien gaat het bij journalisten en advocaten om specifieke groepen en nauwkeurig bepaalde situaties. De Afdeling concludeert dan ook dat de specifieke eisen die het EHRM aan de bescherming van journalisten en advocaten stelt, als een uitzondering moeten worden gezien op de hoofdregel dat artikel 8 EVRM niet per definitie een voorafgaande rechterlijke beoordeling vereist.

b. *Artikel 13 EVRM: 'effectief' toezicht*

Bij de beoordeling of een stelsel van toezicht op inlichtingen- en veiligheidsdiensten aan artikel 13 EVRM voldoet is van belang of dit stelsel als geheel effectief is. Wil een toetsing aan de vereisten van noodzaak, subsidiariteit en proportionaliteit werkelijk inhoud hebben, dan vergt dat van de toezichthoudende instantie(s) niet alleen juridische kennis en vaardigheid maar ook inzicht in en overzicht van het feitelijk handelen van de diensten. De toetsende instantie moet daartoe structureel inzicht hebben in de wijze van werken van de diensten: wat zij kunnen en wat zij mogen. Dergelijk inzicht kan slechts verworven worden in een langdurige en continue toezichtsrelatie met de diensten.⁵⁸ De toezichthouder moet voorts – wil het toezicht in die relatie werkelijk effectief kunnen zijn – volledige inzage hebben in en onbeperkte toegang hebben tot de informatiesystemen van de diensten. Een effectieve toezichthouder zal derhalve over aanzienlijke informatie- en onderzoeksbevoegdheden moeten beschikken.⁵⁹

Effectief toezicht vereist ook dat alle fasen in de werkzaamheden van de diensten afdoende gecontroleerd kunnen worden. Zo moet er niet alleen toezicht zijn op de besluitvorming over de inzet van met name de bijzondere bevoegdheden (de toestemming), maar ook op de feitelijke uitvoering. Dat geldt te meer omdat het toezicht met de toepassing van moderne technologieën complexer en veelomvattender wordt. De verschillende fases waarin gegevens worden verzameld, geselecteerd en verwerkt zijn in de praktijk nauw met elkaar verweven. Het gaat vaak om een continue proces van verwerving, selectie, analyse en onderzoek van gegevens waarbij de verschillende fases, afhankelijk van de

⁵⁸ Venice Commission, *Report on the democratic oversight of security services*, 2015 (Venice Commission 2015b), par. 90: 'Basically, however, security officials make a value judgment on the available information as to whether a particular person is a security risk, and if so, what exactly he or she is up to. It is a question of risk assessment, and this inevitably involves a large degree of subjectivity. Obviously, it takes a long time for any external monitoring body to penetrate the arcane world of intelligence, to understand what is a "reliable" intelligence assessment, and why this is so. Unless and until they are in a position to make a reasonably informed "second assessment", a monitoring body is not a real safeguard.'

⁵⁹ Venice Commission 2015b, par. 125: 'In conclusion on expert oversight bodies, it is important to stress that these must have unrestricted access to the personal information contained in the signals intelligence agency's databanks if they are to be a meaningful safeguard. [...] While an expert body in this respect mainly functions to check that the signal intelligence agencies' own routines on minimisation etc. are functioning correctly, to undertake this task they must have their own, residual, investigative capability, preferably (as with the Dutch and Swedish oversight bodies) having direct access to databanks holding personal information.'

opbrengsten, steeds opnieuw doorlopen kunnen worden (zie hierover punt 4). Dit vraagt om een sterke toezichthouder die zicht heeft op het grote geheel en op de samenhang tussen de verschillende onderdelen van de werkzaamheden van de diensten.

Bij de beoordeling van de rechtmatigheid van de toestemming is het derhalve noodzakelijk dat de toezichthouder voldoende inzicht heeft in de werkwijze van de diensten en de mogelijke effecten daarvan, omdat slechts door kennis te hebben van de concrete uitvoeringspraktijk een op ervaring gebaseerd beoordelingsvermogen opgebouwd kan worden met betrekking tot de potentiële uitwerking van de besluitvorming in de praktijk, waarbij het steeds zal gaan om inschatting van risico's.⁶⁰ Bovendien is een sluitend stelsel van toezicht noodzakelijk omdat de Straatsburgse jurisprudentie vereist dat er een vorm van onafhankelijk toezicht is op de wijze waarop de diensten de aan hen verleende machtiging implementeren en of zij blijven binnen de marges van de verleende toestemming, en meer in het algemeen binnen de marges van subsidiariteit en proportionaliteit.⁶¹

In het licht van het voorgaande gaat de Afdeling hierna eerst in op de vraag of de voorgestelde toetsing door de TIB voldoende bijdraagt aan de effectiviteit van het toezicht. Daarna komt de vraag aan de orde of daar niet beter op andere wijze in kan worden voorzien.

c. *De effectiviteit van de toetsing door de TIB*

De Afdeling is niet overtuigd van de effectiviteit van de toetsing door de TIB. Deze toetsing zal in de praktijk neerkomen op een zeer marginale en abstracte rechtmatigheidsbeoordeling *ex ante*. Omdat de TIB in beginsel alleen betrokken wordt aan de voorkant van het proces, geen rechtstreekse toegang heeft tot de gegevens van de diensten⁶² en slechts beschikt over een beperkte capaciteit, heeft zij niet het benodigde inzicht in en overzicht over de gevolgen van de uitvoeringspraktijk en daarmee over de proportionaliteit van de inzet van de verschillende bevoegdheden. De daarvoor benodigde expertise en capaciteit zit wel bij de CTIVD.⁶³

⁶⁰ Venice Commission 2015b, par. 90.

⁶¹ EHRM 28 juni 2007, 62540/00, Association for European Integration and Human Rights en Ekimdzhiev t. Bulgarije, par. 85-87; EHRM 10 februari 2009, 25198/02, Iordachi e.a. t. Moldavië, par. 41-42. Zie nader hierover het Leidse rapport *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten* (2015), blz. 13-15.

⁶² Zie de toelichting, paragraaf 3.3.3.3: 'Anders dan de CTIVD heeft de TIB geen rechtstreekse toegang tot de gegevens bij de AIVD en MIVD; dat is ook niet nodig nu de taak van de TIB zich – anders dan de CTIVD – beperkt tot een rechtmatigheidstoets op een voorgelegd verzoek'. Hierbij moet de minister weliswaar de TIB alle informatie verschaffen die ten grondslag ligt aan de last, maar de TIB krijgt niet de bevoegdheid die de CTIVD heeft om op eigen beweging in de systemen van de diensten onderzoek te kunnen doen.

⁶³ Zij het dat met de voorgestelde uitbreiding van de bevoegdheden ook de CTIVD versterking behoeft. Zie hierna punt d.

Het ligt gelet op het bovenstaande dan ook in de rede dat de toets door de TIB nagenoeg altijd positief zal uitvallen.⁶⁴ Dat is begrijpelijk, gezien de – mogelijk desastreuze – veiligheidsrisico's die het weigeren van goedkeuring met zich kan brengen. Dat zal des te meer gelden, waar het gaat om de inzet van bevoegdheden die niet zozeer zien op gerichte, afgebakende vormen van interceptie, maar op grootschalige, abstract aangeduide en technisch complexe operaties⁶⁵, waarbij de veiligheidsrisico's enerzijds en de noodzaak, evenredigheid en subsidiariteit van die operaties in het licht van de inbreuken op de persoonlijke levenssfeer anderzijds voor een relatieve buitenstaander zeer moeilijk in te schatten zijn. Het is dan ook waarschijnlijk dat de TIB 'het zekere voor het onzekere' zal nemen en standaard toestemming zal verlenen. In de praktijk zal dat betekenen dat de TIB – onbedoeld – een alibi-functie zal vervullen.

Daar komt nog bij dat met de introductie van de rechtmatigheidstoets van de TIB afbreuk kan worden gedaan aan de ministeriële verantwoordelijkheid voor het handelen van de diensten. De toelichting motiveert de stelling dat dit op geen enkele wijze het geval is, door onder meer te verwijzen naar vergelijkend onderzoek naar de wetgeving van andere landen.⁶⁶ Deze motivering is voorshands niet overtuigend. Ten eerste kent ieder land een eigen stelsel van parlementaire verantwoording; een vergelijking met andere landen heeft niet zonder meer betekenis voor de Nederlandse situatie. Daarnaast valt moeilijk in te zien dat een bindende juridische toets vooraf door een onafhankelijk orgaan geen invloed zou hebben op de verantwoordelijkheid van de minister. Een bindende toets betekent onvermijdelijk een inperking van de ministeriële bevoegdheid en daarmee ook een inperking van de ministeriële verantwoordelijkheid en de daarmee samenhangende mogelijkheid tot parlementaire controle. Bovendien wijst de Afdeling erop dat de beslissing om de diensten een onderzoek te laten starten niet uitsluitend een juridisch oordeel vereist, maar samenhangt met beleidsmatige afwegingen waarbij politieke en internationale componenten een rol spelen; afwegingen die de proportionaliteits- en subsidiariteitstoets kleuren. Onder die omstandigheden ligt het in de rede om het eindoordeel bij de minister te leggen en niet bij een onafhankelijke instantie als de TIB.

De Afdeling onderkent dat het wetsvoorstel met de invoering van de TIB althans in formele zin voldoet aan de jurisprudentie van het EHRM, waar het gaat om de daarin geformuleerde wenselijkheid van een voorafgaande, onafhankelijke en bindende juridische toetsing. Op de hiervoor genoemde materiële gronden – ontleend aan het vereiste van daadwerkelijke effectiviteit van het toezicht – meent de Afdeling deze keuze evenwel ernstig te moeten ontraden. Naar haar oordeel zal een gespecialiseerde instantie – niet alleen bestaande uit juristen, maar ook uit veiligheidsexperts en ict-deskundigen – welke toezicht houdt zowel op de toestemming voor de inzet van interceptiebevoegdheden als op de feitelijke

⁶⁴ Zie de voorbeelden genoemd door Dessens 2013, blz. 97-98.

⁶⁵ Dat geldt bij uitstek voor de inzet van de (nieuwe) bevoegdheden tot onderzoeksopdrachtgerichte kabelgebonden interceptie (artikelen 47-49 van het voorstel).

⁶⁶ Toelichting, paragraaf 9.2.1 Toetskader artikel 8 EVRM, *Voorzienbaarheid: de toestemmingssystematiek*.

uitvoering daarvan en die daardoor zicht heeft op en inzicht heeft in het samenhangende geheel van werkzaamheden van de diensten, in zijn functioneren als toezichthouder beduidend effectiever zijn dan de TIB.

Daarbij komt dat het naast elkaar bestaan van de TIB en de CTIVD de vraag oproept hoe de werkzaamheden van beide organen op elkaar moeten worden afgestemd. Niet uitgesloten is dat TIB en CTIVD op verschillende momenten tot verschillende oordelen komen over de rechtmatigheid van een interceptie of gegevensverwerking. Naar de overtuiging van de Afdeling leidt het voorgestelde systeem met verschillende toezichthouders tot een te gefragmenteerd stelsel dat afbreuk doet aan de vereiste effectiviteit van het toezicht.

d. *Effectiviteit van het toezicht door de CTIVD*

Het ligt gelet op het bovenstaande meer voor de hand om de CTIVD, de huidige toezichthouder, als de gespecialiseerde instantie aan te wijzen die toezicht houdt over het geheel. De CTIVD beschikt al over vergaande onderzoeksbevoegdheden, en heeft zicht op de praktijk van de diensten. Zij geeft rechtmatigheidsoordelen inzake het optreden van de diensten, zowel met betrekking tot de ministeriële toestemming als met betrekking tot de uitvoeringspraktijk. Deze oordelen worden meestal opgevolgd, al zijn ze niet bindend.

Wel zal moeten worden gewaarborgd dat de CTIVD in het licht van de uitbreiding van de bevoegdheden van de diensten (met name de bevoegdheid tot grootscheepse data interceptie en verwerking) beschikt over voldoende expertise en middelen.⁶⁷ Een verdere uitbouw van de CTIVD is daartoe noodzakelijk. Daarbij moet uiteraard allereerst worden gedacht aan de personele invulling van de CTIVD en zijn ondersteunende staf, waarbij naast juridische deskundigheid ook technische deskundigheid en inzicht in veiligheidsrisico's geborgd moet zijn. Voorts is ook van belang dat de CTIVD beschikt over technische voorzieningen die haar in staat stellen om op afdoende wijze te controleren of de toepassing van bevoegdheden door de diensten proportioneel is.⁶⁸

Om te komen tot een effectief stelsel van toezicht acht de Afdeling het noodzakelijk dat, indien gekozen wordt voor het neerleggen hiervan bij de CTIVD, deze allereerst de conceptlasten ter beoordeling voorgelegd krijgt. Daarnaast zal de CTIVD zijn reeds bestaande toezichtstaak op de daarop volgende uitvoering van de lasten door de diensten moeten blijven vervullen. Ingevolge de jurisprudentie van het EHRM, maar ook omwille van het opbouwen van noodzakelijke expertise, moet het toezicht immers niet alleen zien op de rechtmatigheid van de beslissingen om

⁶⁷ Op dit moment beschikt de CTIVD over 3 leden, een staf van 8 medewerkers en 2 secretaresses. Haar begroting bedraagt 1,5 miljoen euro. Ter vergelijking: de begroting van de Algemene inlichtingen- en veiligheidsdienst bedraagt over 2017 212,7 miljoen euro (zie Miljoenennota 2017), die van de Militaire inlichtingen- en veiligheidsdienst 90 miljoen euro. Vgl. ook Kamerstukken II 2014/15, 29 754, nr. 302.

⁶⁸ Zie de Privacy Impact Assessment van 12 februari 2016, blz. 146 en de reactie van dr. J.V.J. van Hoboken en dr. M.R. Koot van 29 augustus 2015 op de consultatieversie.

bevoegdheden in te zetten (de ministeriële lasten), maar ook op de daadwerkelijke tenuitvoerlegging daarvan.

Vervolgens moet worden gezien of de oordelen van de CTIVD over de last en over de uitvoering daarvan bindend zouden moeten zijn. Voor het standpunt dat de regering in het consultatiewetsvoorstel heeft ingenomen om dat oordeel niet bindend te laten zijn, pleiten de hiervoor al genoemde overwegingen, die er samengevat op neerkomen dat daarmee de ministeriële verantwoordelijkheid en de verantwoordingsplicht jegens het parlement beter tot hun recht komen. De Afdeling wijst er op dat de inzet van de diensten inherent verweven is met complexe risico-inschattingen, waarbij beleidsmatige afwegingen met politieke en internationale componenten een grote rol spelen. Bij dergelijke beoordelingen is het gewenst dat uiteindelijk de verantwoordelijke minister de knoop doorhakt en daarover met name in lastige kwesties aan het parlement (zo nodig vertrouwelijk in verband met de noodzakelijke geheimhouding) verantwoording aflegt.⁶⁹

In dit kader zou wel sprake moeten zijn van een (reeds eerder in het consultatiewetsvoorstel voorgestelde) heroverwegingsplicht, waarbij de minister slechts op *zwaarwegende gronden* kan besluiten de last in afwijking van het oordeel van de CTIVD ongewijzigd te handhaven. In die gevallen – waarbij het gaat om zeer uitzonderlijke situaties – zou de minister tevens het parlement zo spoedig mogelijk in kennis moeten stellen van zijn besluit onder mededeling van die gronden en van het oordeel van de CTIVD,⁷⁰ voor zover het verstrekken van de desbetreffende stukken niet in strijd is met het belang van de staat, in welk geval vertrouwelijke mededeling plaats zou dienen te vinden. Eenzelfde heroverwegingsprocedure zou plaats dienen te vinden bij de beoordeling van de uitvoeringspraktijk van de diensten.⁷¹ De CTIVD zou ten aanzien daarvan de bevoegdheid moeten krijgen te oordelen dat een bepaalde operatie, interceptie of wijze van uitvoering onrechtmatig is, welk oordeel de minister slechts op zwaarwegende gronden naast zich neer zou mogen leggen, waarbij een soortgelijke informatieverplichting jegens het parlement van toepassing zou moeten zijn. Het wetsvoorstel zou hiervoor een regeling moeten bevatten.

De hier geschetste inrichting van toezicht door de CTIVD over het geheel van activiteiten van de diensten is beduidend effectiever dan een juridische ex ante toetsing door de TIB. Hiermee is weliswaar geen sprake van een bindend – in

⁶⁹ Zie aldus de regering in het kader van het wetsvoorstel tot wijziging van artikel 13 Grondwet, waarin de nationale veiligheid de uitzondering vormt op het vereiste van een rechterlijke machtiging bij inbreuken op persoonlijke communicatie, waarin zij stelde dat 'de keuze om in deze gevallen een machtiging van de Minister in plaats van de rechter te eisen samenhangt met de verantwoordelijkheid van de Minister, omdat het gaat om belangrijke beleidsbeslissingen die verband houden met de nationale veiligheid. Deze argumentatie is onverkort valide' (Kamerstukken II 2013/14, 33 989, nr. 3, blz. 27). Deze argumentatie is ook valide ten aanzien van een niet-rechterlijke onafhankelijke instantie zoals de CTIVD.

⁷⁰ Aldus was voorgesteld in artikel 102 van het consultatiewetsvoorstel. Zie voor een vergelijkbare regeling artikel 128, zesde lid, Wet op de rechterlijke organisatie.

⁷¹ Daarbij is het overigens onvermijdelijk dat de CTIVD slechts steekproefsgewijs die praktijk zal kunnen onderzoeken.

principe rechterlijk – toezicht, waarvoor het EHRM een voorkeur heeft uitgesproken. Het Hof heeft in de zaak *Kennedy* evenwel aanvaard dat ook niet-bindend toezicht door de *Interception of Communications Commissioner* (te samen overigens met bindend klachtrecht achteraf bij de Investigatory Powers Tribunal (IPT)⁷²) in het licht van het EVRM voldoet.⁷³ Daarbij moet in ogenschouw genomen worden dat de positie van de CTIVD zoals hier voorgesteld beduidend sterker is dan die van de *Commissioner*. Bovendien zij er op gewezen dat de huidige, niet-bindende adviezen van de CTIVD doorgaans door de ministers worden opgevolgd.⁷⁴

e. *Klachtrecht*

De behandeling van klachten is in de huidige Wiv 2002 belegd bij de Nationale ombudsman.⁷⁵ Het wetsvoorstel past de bestaande regeling voor klachtbehandeling aan. Het geeft burgers de mogelijkheid om bij de CTIVD een klacht in te dienen over de werkwijze van de diensten. Voor de behandeling van klachten wordt bij de CTIVD een afdeling klachtbehandeling ingesteld, die strikt gescheiden is van de afdeling toezicht. Deze afdeling krijgt de bevoegdheid om naar aanleiding van een klacht een bindende uitspraak te doen. Het bestaan van een klachtvoorziening vormt een sluitstuk in het stelsel van toezicht op de inlichtingen- en veiligheidsdiensten. De regering merkt op dat zij in het licht daarvan naar aanleiding van de ontwikkeling in de jurisprudentie van het EHRM en in navolging van de aanbeveling van de Commissie Dessens tot de voorgestelde regeling voor klachtbehandeling heeft besloten. In de toelichting wordt deze klachtregeling dan ook nadrukkelijk gemotiveerd tegen de achtergrond van artikel 13 EVRM: het recht op een effectief en daadwerkelijk rechtsmiddel.⁷⁶

Ook in het oorspronkelijke ontwerp voor de Wiv 2002, zoals dat in 1996 aan de Raad van State werd voorgelegd, wilde de regering de CTIVD als externe klachtbehandelaar aanwijzen. De Raad adviseerde destijds om de klachtbehandeling bij de Nationale ombudsman te laten. Klachtbehandeling door de CTIVD zou volgens de Raad misschien effectiever zijn, maar “daar staat onvermijdelijk een dreigend verlies aan objectiviteit en onafhankelijkheid tegenover. Een klacht over de handelwijze of bejegening door een dienst zal immers het – integrale – toezicht daarop impliceren. Met andere woorden: indien een klacht gegrond is, heeft ook de toezichthouder gefaald, tenzij deze redelijkerwijs niets te verwijten valt. Reeds om deze reden dienen toezicht en onafhankelijke klachtbehandeling strikt gescheiden te zijn, opdat zelfs de schijn van partijdigheid

⁷² Waaroever hierna meer in punt e.

⁷³ EHRM 18 mei 2010, 26839/05, *Kennedy* t. Verenigd Koninkrijk, par. 155-170. Het aantal klachten bij IPT dat gegrond verklaard wordt is overigens zeer gering: in de periode 2000-2012 in 5 van de 1468 klachten.

⁷⁴ Aldus Dessens 2013, blz. 101. Zie CTIVD-toezichtsrapport nr. 30b (2012) blz. 5, voor enkele spaarzame voorbeelden waarin de minister van het advies afweek.

⁷⁵ Artikelen 83 en 84 Wiv 2002. De CTIVD heeft in de bestaande klachtprocedure een adviesrecht en functioneert aldus als een interne klachtcommissie, met enkele waarborgen voor een verdergaande onafhankelijkheid ten opzichte van de minister dan dergelijke interne klachtcommissies over het algemeen hebben.

⁷⁶ Toelichting paragraaf 9.5.

wordt vermeden.”⁷⁷ De Afdeling acht deze overwegingen ook met betrekking tot het thans voorliggende voorstel nog steeds geldig.

De motivering voor de introductie van een bindende klachtbevoegdheid bij de CTIVD is blijkens de toelichting vooral gebaseerd op het arrest van het EHRM in *Segerstedt-Wiberg tegen Zweden*.⁷⁸ Dit arrest zag evenwel uitsluitend op de opslag, inzage en vernietiging van door de Zweedse veiligheidsdienst opgeslagen gegevens met betrekking tot klagers en de afwezigheid van enig rechtsmiddel om inzage en vernietiging van die gegevens af te dwingen.

In dit verband benadrukt de Afdeling nogmaals dat het EHRM de vraag of in een verdragsstaat sprake is van een daadwerkelijk rechtsmiddel steeds op basis van alle beschikbare voorzieningen gezamenlijk beoordeelt. Dat wil zeggen dat als één van de in een verdragsstaat aanwezige voorzieningen voor klachtbehandeling niet voldoet aan de hierboven weergegeven eisen, niet per definitie sprake is van een schending van artikel 13 van het EVRM.⁷⁹ In dit licht bezien acht de Afdeling de conclusie over het vereiste van bindende oordelen door een klachtinstantie te absoluut en te generiek. De toereikendheid van de vormgeving van het klachtrecht kan alleen beoordeeld worden tegen de achtergrond van het gehele toezichtskader voor de inlichtingen- en veiligheidsdiensten. Daartoe behoren ook de bepalingen inzake het recht op inzage en correctie⁸⁰ met bijbehorende bestuursrechtelijke rechtsbescherming. Voor zover deze bepalingen onvoldoende inzage- en correctierecht zouden bieden ligt het veeleer voor de hand deze aan te passen.⁸¹ Daar komt bij dat het laatste oordeel over de rechtmatigheid van de procedure en de inzet van de bevoegdheden aan de rechter is.⁸² Mede gezien deze aanvullende mogelijkheden voor burgers om klachten over de inzet van de bevoegdheden door de diensten voor te leggen aan een rechterlijke instantie die hierover bindende uitspraken kan doen wordt voldaan aan artikel 13 EVRM. Tegen deze achtergrond kan niet geconcludeerd worden dat het ontbreken van bindende oordelen in klachtzaken door een andere instantie dan de rechter onverenigbaar is met de eisen die het EVRM stelt aan toezicht.

⁷⁷ Advies van 17 september 1997, Kamerstukken II 1997/98, 25 877, A.

⁷⁸ EHRM 6 juni 2006, no. 62332/00, *Segerstedt-Wiberg e.a. t. Zweden*, § 118. Daarnaast wordt verwezen naar het eerdere arrest EHRM 26 maart 1987, no. 9248/81, *Leander t. Zweden*, dat evenzo betrekking had op de weigering van toegang tot gegevens inzake de betrokkene op grond van nationale veiligheid en het gebrek aan rechtsmiddelen ter zake. Ook het rapport van de Universiteit Leiden baseert zijn conclusies over de eis van bindendheid in klachtzaken hoofdzakelijk op deze beide Zweedse zaken.

⁷⁹ Toelichting, paragraaf 9.5.

⁸⁰ De artikelen 47-56 van de Wiv 2002, respectievelijk de artikelen 74-83 van het voorstel.

⁸¹ Een klacht over niet-openbaarmaking onder het eerdere regime, waarbij de Wet openbaarheid van bestuur van toepassing was, werd door het Hof niet ontvankelijk verklaard: EHRM 5 april 2005, 9940/04, *Brinks t. Nederland*. De huidige regeling bevat beduidend meer weigeringsgronden dan de Wob (grosso modo geïncorporeerd in artikelen 82 en 83 van het voorstel resp. artikelen 55 en 56 Wiv 2002), zie artikel 80 van het voorstel resp. artikel 53 Wiv 2002.

⁸² Zie toelichting, paragraaf 7.3.4. Vgl. in dit verband Rb. Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436 en Hof Den Haag 27 oktober 2015, ECLI:NL:GDHA:2015:2881 inzake het zonder rechterlijke machtiging ‘tappen’ van advocaten. Zie over de relevantie van de gang naar de rechter: EHRM 6 september 1978, 5029/71, *Klass e.a. t. Duitsland*, par. 71.

Ten slotte moet het feitelijke belang van het klachtrecht in proportie gezien worden. De CTIVD, die in de bestaande klachtprocedure advies aan de minister geeft en functioneert als een interne klachtcommissie, behandelt per jaar zo'n 10-15 klachten.⁸³ De daarop volgende klachtprocedures bij de Ombudsman zijn qua aantal nog beperkter: gemiddeld 2 per jaar inzake de AIVD, en 1 per jaar inzake de MIVD. Het komt de Afdeling al met al voor dat investering in de uitbouw van de toezichtstaak van de CTIVD zinvoller is dan het optuigen van een zelfstandige afdeling klachtbehandeling.

f. *Conclusie*

Op grond van het bovenstaande acht de Afdeling het voorgestelde stelsel van toezicht als geheel niet toereikend. Hoewel de Afdeling onderkent dat met de introductie van voorafgaande toetsing door de TIB tegemoet wordt gekomen aan de voorkeur van het EHRM voor een bindende juridische toetsing vooraf, komt zij tot de conclusie dat hierdoor het stelsel van toezicht op de inzet van de diensten en de wijze waarop zij hun bevoegdheden uitoefenen in het geheel gezien onvoldoende effectief zal zijn. Toetsing door de TIB zal in de praktijk neerkomen op een marginale en abstracte rechtmatigheidsbeoordeling *ex ante*. Daarbij komt dat het als gevolg van het wetsvoorstel naast elkaar bestaan van de TIB en de CTIVD in verband met de daaruit voortvloeiende afstemmingsproblemen gemakkelijk afbreuk kan doen aan de effectiviteit van het toezicht. Om deze reden meent de Afdeling dat het wetsvoorstel op dit punt niet in de huidige vorm aan de Tweede Kamer voorgelegd dient te worden.

Het ligt veeleer in de rede om het toezicht bij de CTIVD te concentreren. In tegenstelling tot de TIB beschikt de CTIVD niet alleen over juridische kennis maar heeft zij ook inzicht in en overzicht van het daadwerkelijk handelen van de diensten. Het neerleggen van de toetsing *ex ante* en *ex post* bij de CTIVD, met een regeling inzake een verzwaarde plicht tot heroverweging, betekent daarnaast dat het parlement de concrete mogelijkheid heeft om de minister aan de hand van het oordeel van de CTIVD ter verantwoording te roepen over die inzet en uitvoering door de diensten waar twijfel gerezen is over de rechtmatigheid ervan. De Afdeling adviseert in het licht van het bovenstaande af te zien van de introductie van de TIB en het voorstel aan te passen.

Mede in het licht van de wenselijkheid om het toezicht in handen te leggen van de CTIVD meent de Afdeling dat de klachtbehandeling niet door de CTIVD zou moeten plaatsvinden. Een klacht over de handelwijze of bejegening door een dienst zal immers het – integrale – toezicht daarop impliceren. Reeds om deze reden dienen toezicht en onafhankelijke klachtbehandeling strikt gescheiden te zijn, opdat zelfs de schijn van partijdigheid wordt vermeden. Gelet daarop adviseert de Afdeling de klachtregeling zoals thans in de Wiv 2002 neergelegd ongewijzigd te laten.

⁸³ Zo blijkt uit de jaarverslagen van de CTIVD dat deze in 2013 18 klachten behandelde, in 2014 10 en in 2015 9.

4. Gegevensverwerking: Big Data

a. *Het belang en de risico's van Big Data*

De toelichting wijst er terecht op dat de snelle opkomst en mondiale verspreiding van digitale technologie en het internet vergaande gevolgen heeft. De technologische ontwikkeling heeft ook ingrijpende gevolgen voor het functioneren van de inlichtingen- en veiligheidsdiensten. Deze diensten dienen adequaat op deze ontwikkeling te kunnen inspelen en met het oog daarop de bevoegdheden en middelen te hebben om hun taken in de huidige tijd te kunnen uitvoeren. In de toelichting wordt op overtuigende wijze aangetoond dat de voorgestelde uitbreiding van bevoegdheden, met inbegrip van de in artikelen 47-49 geregelde bevoegdheden tot onderzoeksopdrachtgerichte interceptie, noodzakelijk is opdat de diensten ook in de nabije toekomst een effectieve bijdrage kunnen leveren aan het voorkomen en bestrijden van de terroristische, militaire en technologische dreigingen waar de hedendaagse samenleving mee geconfronteerd wordt.

Voor het adequaat functioneren van de diensten is bevoegdheidsuitbreiding evenwel niet voldoende. Daarvoor is ook essentieel dat het optreden van de inlichtingen- en veiligheidsdiensten met effectieve waarborgen is omgeven. De diensten dienen ook in de toekomst het vertrouwen te genieten van de burgers en degenen die hen in het parlement vertegenwoordigen, dat zij op integere wijze en met inachtneming van rechtsstatelijke waarborgen hun wettelijke taak uitvoeren. De onthullingen van Edward Snowden over de massasurveillance door de Amerikaanse National Security Agency (NSA) en het politieke en maatschappelijke debat dat daarover ook in Nederland is ontstaan, heeft aangetoond dat dat vertrouwen niet vanzelfsprekend is en onder alle omstandigheden behouden kan blijven. Aan dat debat draagt bij dat de technische mogelijkheden voor de diensten om informatie te verzamelen en te verwerken in korte tijd exponentieel zijn toegenomen, in combinatie met het feit dat de werkzaamheden van de diensten uit de aard der zaak grotendeels aan de publieke waarneming zijn onttrokken.

Om het politieke en maatschappelijke vertrouwen van de diensten blijvend te kunnen behouden is van cruciaal belang om te bepalen hoe de wijze waarop de noodzakelijke bevoegdheidsuitbreiding in het wetsvoorstel is vormgegeven en deze in de praktijk haar beslag gaat krijgen, zich in bredere zin verhoudt tot de geschetste technologische ontwikkelingen. De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) heeft in zijn recente rapport *Big Data in een vrije en veilige samenleving* de kansen en risico's van de huidige technische mogelijkheden om op grote schaal gegevens te analyseren en te gebruiken, in kaart gebracht. Daarbij gaat het om zogeheten 'Big Data': grote hoeveelheden gestructureerde en ongestructureerde data die uit verschillende bronnen afkomstig zijn en die op geautomatiseerde wijze op mogelijke correlaties kunnen worden doorzocht en geanalyseerd. Deze analyses leiden tot kennis die tot dusverre vaak niet

beschikbaar was en die de basis kunnen zijn voor innovatief overheidsoptreden in onder meer het veiligheidsdomein.⁸⁴

Het gebruik van Big Data heeft, zo wordt ook door de WRR onderstreept, een grote potentie.⁸⁵ Dat komt vooral omdat veel data tegenwoordig automatisch worden geproduceerd en het onvermijdelijke bijproduct zijn van dagelijkse handelingen van bijna alle burgers, zoals het gebruik van internet, sociale media, mobiele telefoons en daaraan verbonden applicaties. Hierdoor worden steeds meer handelingen van individuen digitaal geregistreerd. De geautomatiseerde analyse van deze gegevens in hun onderlinge samenhang kan een schat aan informatie opleveren. Toepassing van deze technieken levert grote tijdswinst op en kan – mits de analyses zorgvuldig worden uitgevoerd – tot nauwkeurige en geïndividualiseerde resultaten leiden. Daardoor kunnen overheden – en met name de inlichtingen- en veiligheidsdiensten – veel sneller en gericht inspelen op bepaalde gebeurtenissen die hebben plaatsgevonden of mogelijk nog zullen plaatsvinden. Aanslagen kunnen met het oog op toekomstige dreigingen sneller en beter worden gereconstrueerd, terroristische netwerken beter en sneller in kaart gebracht. Hoewel de effectiviteit van de gebruikte analysemethoden nog niet altijd aantoonbaar is, worden al positieve resultaten geboekt. Verwacht mag worden dat dit soort toepassingen in de nabije toekomst steeds belangrijker zal worden.

De WRR wijst echter ook op de risico's.⁸⁶ De grootschalige verzameling, opslag en analyse van gegevens door de overheid, en met name door de inlichtingen- en veiligheidsdiensten, kunnen ertoe leiden dat burgers het gevoel krijgen dat hun vrijheid en meer in het bijzonder hun persoonlijke levenssfeer wordt aangetast. Als reactie daarop zullen zij vervolgens hun gedrag gaan aanpassen ('chilling effect'). Dat gevoel wordt versterkt doordat de methoden en technieken van gegevensverwerking die door de overheid worden gebruikt voor de burger nauwelijks inzichtelijk en navolgbaar zijn. Big Data-toepassingen kunnen ook leiden tot categorisering en profilering van groepen burgers met – zonder rekening te houden met individuele omstandigheden – mogelijk onevenredige gevolgen alsook discriminatie en oneerlijke behandeling. Het feit dat data-analyses fouten kunnen bevatten en kunnen leiden tot verkeerde conclusies (gevonden statistische correlaties wijzen bijvoorbeeld niet zonder meer op een causaal verband) hangt hiermee samen.⁸⁷ Tot slot wijst de WRR op het risico van 'function creep': Big Data-toepassingen maken het aanzienlijk gemakkelijker om gegevens te gebruiken voor een ander doel dan waarvoor de data oorspronkelijk zijn verzameld. Sterker nog, de grote meerwaarde van deze toepassingen zit juist in een aanzienlijke vergroting van de mogelijkheid tot secundair gebruik van gegevens.

Deze technologische ontwikkelingen lijken vergaande gevolgen te gaan hebben voor de wetgeving en voor de basisprincipes die daaraan ten grondslag liggen. Er

⁸⁴ WRR, *Big Data in een vrije en veilige samenleving*, Amsterdam University Press, Den Haag/Amsterdam 2016 (hierna: WRR 2016), blz. 21.

⁸⁵ WRR 2016, blz. 76 e.v.

⁸⁶ WRR 2016, blz. 88.

⁸⁷ WRR 2016, blz. 82.

tekent zich een fundamentele verschuiving af, waarbij de aandacht in het proces van gegevensverwerking voor het verzamelen van gegevens verschuift naar de analyse en het gebruik daarvan. De WRR wijst er terecht op dat hierdoor de traditionele beginselen van doelbinding en noodzakelijkheid zoals deze in de huidige wetgeving inzake gegevensbescherming zijn neergelegd onder druk komen te staan. Dit roept de vraag op of aanpassing en/of aanvulling van dat kader noodzakelijk is. De WRR heeft deze vraag bevestigend beantwoord: alleen door extra eisen te stellen aan het toepassen van Big Data-analyses kan het vertrouwen worden gecreëerd en bevestigd dat de overheid niet sluipenderwijs doordringt in de persoonlijke vrijheid van burgers.⁸⁸

In de rechtspraak is toenemende aandacht voor bescherming van fundamentele rechten die samenhangen met gebruik van moderne technieken. In 2014 heeft het Hof van Justitie van de Europese Unie de Dataretentierichtlijn (Richtlijn 2006/24/EG), die bepaalde dat telecomaandbieders moeten worden verplicht om met het oog op de opsporing van zware criminaliteit verkeersgegevens op te slaan, ongeldig verklaard omdat deze 'een zeer ruime en bijzonder zware inmenging' inhield van het recht op bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens als bedoeld in artikel 7 en 8 EU-Handvest voor de grondrechten.⁸⁹ Dat oordeel was gebaseerd op het in de richtlijn ontbreken van belangrijke waarborgen, niet alleen met betrekking tot het verzamelen, maar ook met betrekking tot het gebruik (bewaren en raadplegen) van de bewaarde gegevens. In dat verband wees het Hof er onder meer op dat de richtlijn van toepassing was op alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, zonder enige relatie met het doel van de gegevensverzameling (in casu het bestrijden van zware criminaliteit) en zonder dat er enige aanwijzing bestond dat het gedrag van degenen wier gegevens geregistreerd worden enig verband vertoonde met zware criminaliteit.⁹⁰ Deze strenge koers van het Hof van Justitie met het oog op de bescherming van persoonsgegevens is in latere arresten voortgezet.⁹¹ Hoewel het EU-recht en de rechtspraak van het Hof niet van toepassing zijn op de diensten,⁹² is aannemelijk dat de daarin geformuleerde uitgangspunten ook voor de reikwijdte en begrenzing van hun bevoegdheden betekenis hebben. Deze betekenis zal met name gestalte kunnen krijgen door verdere doorwerking van de rechtspraak van het Luxemburgse Hof in die van het EHRM.⁹³ Overigens heeft het EHRM zich de afgelopen jaren in het kader van de toetsing aan artikel 8 EVRM reeds kritisch getoond in gevallen waarin de overheid

⁸⁸ WRR 2016, blz. 137.

⁸⁹ HvJEU 8 april 2014 (ECLI:EU:C:2014:238) in de gevoegde zaken C-293/12 (Digital Rights Ireland tegen Ierland) en C-594-12 (Seitlinger, Tschohl e.a. tegen Kärntner Landesregierung).

⁹⁰ Digital Rights Ireland, punten 57-59.

⁹¹ HvJEU 13 mei 2014, ECLI:EU:C:2014:317, C-131/12 (Google Spain tegen Agencia Espanola de Protección (AEPD), Mario Costeja González) en HvJEU 6 oktober 2015, ECLI:EU:C:2015:650, C-362/14 (Maximillian Schrems tegen Data Protection Commissioner).

⁹² Zie de artikelen 72 en 276 van het VWEU.

⁹³ 'Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten', Universiteit Leiden, bijlage bij de reactie van de CTIVD op het conceptwetsvoorstel Wiv 20xx, blz. 23. Vgl. de verwijzing naar Digital Rights Ireland in EHRM 12 januari 2016, 37138/14, Szabo en Vissy t. Hongarije, par. 70.

ongedifferentieerde en allesomvattende intercepties mag plegen en persoonsgegevens mag opslaan en raadplegen.⁹⁴

In het licht van het voorgaande merkt de Afdeling het volgende op.

b. *Een samenhangende visie*

De Afdeling stelt vast dat op verschillende plaatsen in de toelichting uitgebreid wordt ingegaan op de mogelijke gevolgen van de beschikbare moderne technieken en de daarmee samenhangende bevoegdheden in het wetsvoorstel. Daarbij gaat de aandacht vooral uit naar de onderzoeksopdrachtgerichte interceptie (artikelen 47-49). Getracht wordt om per wetsartikel inzichtelijk te maken – soms ondersteund door concrete voorbeelden – in welke gevallen de betreffende bevoegdheid wel en in welke gevallen zij niet mag worden toegepast.⁹⁵

Hoewel de Afdeling waardering heeft voor deze artikelsgewijze toelichting, die in het algemeen helderheid biedt over de betekenis van de afzonderlijke bevoegdheden, mist de Afdeling een algemene beschouwing over de wijze waarop de hiervoor geschetste technologische ontwikkelingen – en in het bijzonder Big Data-toepassingen – doorwerken in het onderhavige wetsvoorstel. Een dergelijke beschouwing acht de Afdeling nodig opdat een beter overzicht ontstaat van het stelsel als geheel zoals neergelegd in het wetsvoorstel en van de samenhang tussen de diverse bevoegdheden en waarborgen.

In die algemene beschouwing zou ingegaan moeten worden op de vraag in hoeverre de technologische ontwikkelingen de werkwijze van de inlichtingen- en veiligheidsdiensten hebben veranderd (meer in het bijzonder in hoeverre ook bij de diensten sprake is van een betekenisvolle verschuiving van verzameling van gegevens naar analyse en gebruik van gegevens) en wat deze veranderingen betekenen voor de algemene oriëntatie van het regelgevingskader. Met betrekking tot het laatste is met name de vraag welke feitelijke betekenis, gegeven de technologische ontwikkelingen, toekomt aan de beginselen van doelbinding en noodzakelijkheid bij Big Data-toepassingen door de diensten, in hoeverre de betekenis van die beginselen daardoor veranderd is en welke aanvullende waarborgen het wetsvoorstel bevat of zou moeten bevatten om de specifiek met het oog op Big Data-toepassingen gepaard gaande risico's het hoofd te bieden.

c. *Transparantie werkwijze*

De WRR heeft in haar eerder genoemde rapport aanbevolen dat er meer transparantie moet komen over de dataverwerkingsprocessen van de overheid.⁹⁶ Voor burgers is ook door de moderne techniek de gegevensverwerking door de

⁹⁴ EHRM 4 december 2008 30562/04 en 30566/04, S. en Marper t. Verenigd Koninkrijk, par. 119; EHRM 18 mei 2010, 26839/05, Kennedy t. Verenigd Koninkrijk, par. 160; EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 302; EHRM 12 januari 2016, 37138/14, Szabo en Vissy t. Hongarije, par. 66-69 en 89.

⁹⁵ Met betrekking tot de onderzoeksopdrachtgerichte interceptie vooral paragraaf 3.3.4.4.7.4 en bijlage 4 van de toelichting.

⁹⁶ WRR 2016, blz. 144.

overheid in veel gevallen een 'black box'. Meer transparantie is gewenst om het vertrouwen in de zorgvuldigheid en proportionaliteit van die gegevensverwerking te waarborgen. Daarbij kunnen onder meer de openbare rapportages van toezichthouders zoals de CTIVD een belangrijke rol spelen. Voorts acht de WRR het wenselijk dat de overheid burgers meer inzicht geeft in de frequentie van de gegevensverzameling, de doelen waarvoor dat gebeurt en – waar mogelijk – welke effecten gegevensanalyses sorteren. Organisaties zouden daartoe in een beleidsplan moeten vastleggen welke Big Data-toepassingen zij gebruiken om uitwerking te geven aan hun wettelijke taken en wat de kosten en de beoogde resultaten daarvan zijn. Vervolgens zou daarover in een later stadium – meer dan thans gebeurt in de jaarverslaglegging – verantwoording moeten worden afgelegd.

Gelet op de aard van de gegevensverwerking door de inlichtingen- en veiligheidsdiensten zal de transparantie aanzienlijk beperkter zijn dan bij andere overheidsorganisaties. De WRR wijst er echter op dat in diverse Europese landen een aanzienlijk grotere mate van openbaarheid over de technieken en operaties van het inlichtingenwerk betracht wordt, zonder dat dit het functioneren van de inlichtingendiensten noemenswaardig belemmert.⁹⁷ In dat verband memoreert de WRR de discussie over de geheimhouding van tapstatistieken.⁹⁸ Tegen deze achtergrond adviseert de Afdeling om uitgebreider⁹⁹ in de toelichting in te gaan op de vraag of en zo ja, op welke wijze de diensten uitvoering kunnen geven aan de aanbevelingen van de WRR en hoe in dat verband het belang van de gewenste transparantie moet worden afgewogen tegen het belang van de noodzakelijke geheimhouding.

d. *Driefasenaanpak en toestemming*

Voor zover het Big Data-toepassingen betreft gaat – zo blijkt ook uit de consultatie – bijzondere aandacht uit naar de bevoegdheid tot onderzoeksopdrachtgerichte interceptie. Blijkens het wetsvoorstel en de toelichting verloopt deze in drie fasen. De eerste fase betreft de doelgerichte verwerving van telecommunicatie (artikel 47). Het gaat hier om het binnenhalen van grote hoeveelheden gegevens (bulkinterceptie). Tot die bevoegdheid behoort ook de bevoegdheid tot het ongedaan maken van de versleuteling van de telecommunicatie of gegevens alsmede de technische analyse van de gegevens voor zover deze gericht is op de optimalisatie van de resultaten van de interceptie. In de tweede fase gaat het om de voorbereiding van de onderschepte gegevens (artikel 48). Het gaat hier om een verkenning van de binnengehaalde gegevens door het vaststellen van de kenmerken en de aard van de telecommunicatie en van de identiteit van de persoon of organisatie die daarbij hoort. De cruciale vraag in deze fase is: wordt datgene onderschept wat beoogd wordt? Tot deze fase behoort ook het vaststellen en verifiëren van de selectiecriteria die de basis vormen voor nader onderzoek. In de derde fase ten slotte vindt de daadwerkelijke selectie van de gegevens plaats en worden deze gebruikt om inzicht te verwerven in de intenties, de capaciteiten en de gedragingen van personen en instanties die onderwerp zijn

⁹⁷ WRR 2016, blz. 145.

⁹⁸ Zie ABRvS 13 januari 2016, nr. 201409649/1A3.

⁹⁹ De toelichting is thans te summier. Zie paragraaf 1.2.2.

van onderzoek (artikel 49). In deze fase kan ook geautomatiseerde data-analyse worden toegepast (artikel 59).¹⁰⁰

In de reactie van de CTIVD op het consultatiewetsvoorstel wordt mede aan de hand van een fictieve casus geïllustreerd dat de drie fases in de praktijk nauw met elkaar verweven zullen zijn en daardoor in de tijd soms veelal niet of nauwelijks van elkaar onderscheiden zullen kunnen worden.¹⁰¹ Het gaat vaak om een continue proces van verwerving, selectie, analyse en onderzoek van gegevens, waarbij de in de toelichting beschreven fases, afhankelijk van de opbrengsten, steeds opnieuw doorlopen kunnen worden. Gelet hierop is aannemelijk dat in veel gevallen niet voor elke fase afzonderlijk de door de artikelen 47 tot en met 49 voorgeschreven toestemming zal worden verleend maar dat doorgaans een gecombineerde last zal worden afgegeven; in een zelfde last zal voor meerdere handelingen uit verschillende fasen tegelijkertijd toestemming worden gegeven. De artikelen 47 tot en met 49 lijken, integendeel, uit te gaan van een zekere volgordeelijkheid, waarbij in elke fase afzonderlijk voor een aantal handelingen toestemming moet worden verleend. Het is evenwel aannemelijk dat in afwijking hiervan in de regel een combi-last zal worden afgegeven, die relatief algemeen en abstract zal zijn geformuleerd¹⁰² en daardoor minder waarborgen zal bieden dan uit het wetsvoorstel zou kunnen worden afgeleid. In de toelichting wordt dit onderkend,¹⁰³ maar de mogelijkheid om een combi-last af te geven is in het wetsvoorstel niet geregeld. Indien een dergelijke combi-last in de praktijk noodzakelijk is, dient het wetsvoorstel hiervoor een duidelijke regeling te bevatten.

De Afdeling adviseert in de toelichting op het bovenstaande in te gaan en het wetsvoorstel zo nodig aan te passen.

e. *Uitwerking onderzoeksoopdrachtgerichte interceptie*

In de toelichting wordt de kritiek op het conceptwetsvoorstel dat de bevoegdheid tot onderzoeksoopdrachtgerichte interceptie (in het wetsvoorstel neergelegd in artikelen 47-49) neer zou komen op een 'sleepnetbevoegdheid', afgewezen. Tegelijkertijd wordt erkend dat met de uitoefening van de bevoegdheid – of dat nu in het niet-kabelgebonden of kabelgebonden domein plaatsvindt – gegevens worden geïntercepteerd van een grote hoeveelheid personen en instanties; dat is inherent aan onderzoeksoopdrachtgerichte interceptie van grote hoeveelheden data.¹⁰⁴ Die ruime schaal is mede nodig omdat het onderzoek ook gericht kan zijn op nog (nagenoeg) ongekennde dreigingen. Daarbij zal de interceptie blijkens de toelichting plaatsvinden op een bepaald onderzoeksgebied of thema (bijvoorbeeld

¹⁰⁰Toelichting, paragraaf 3.3.4.4.7.4.

¹⁰¹Reactie CTIVD, blz. 26 e.v.

¹⁰²Dat lijkt aan te sluiten bij de ervaringen van de CTIVD als het gaat om de toepassing van de selectiebevoegdheid. De CTIVD heeft in het verleden bij herhaling geconstateerd dat bij de selectie sprake is van een grote mate van 'uitproberen': selectie wordt breed ingezet aan de hand van criteria (persoonsgegevens) waarvan de relevantie niet altijd vaststaat. Als gevolg van deze praktijk wordt selectie in veel gevallen door de diensten onvoldoende (concreet) gemotiveerd. Zie de reactie van de CTIVD op het consultatiewetsvoorstel, blz. 31.

¹⁰³Toelichting, paragraaf 3.3.4.4.7.4

¹⁰⁴Toelichting, paragraaf 12.2.

terrorisme of cyberdreigingen) waarbij de diensten zich richten op bijvoorbeeld een geografisch gebied of bepaalde datastromen. Informatie die evident niet relevant is voor een onderzoek dan wel enig ander lopend ander onderzoek in het kader van de taken van de dienst, zal zo spoedig mogelijk worden vernietigd.¹⁰⁵

Omdat gegevens worden onderschept van grote hoeveelheden personen is in de Privacy Impact Assessment (PIA) gesteld dat ook de onderzoeksopdrachtgerichte interceptie zoveel mogelijk toegespitst moet worden op communicatiestromen die het meest relevant voor de diensten zijn, en er zo snel mogelijk een selectie moet plaatsvinden om de nadere verwerking te beperken tot de kring van personen die daadwerkelijk tot het aandachtsveld van de diensten behoren. Een snelle beoordeling op relevantie van gegevens is daarom nodig, gevolgd door het terstond vernietigen van gegevens die niet relevant blijken te zijn, aldus de PIA.¹⁰⁶ Daarbij sluit de PIA aan bij Jacobs, die een twee fasen-model volgens het principe 'select while you collect' heeft voorgesteld.¹⁰⁷ In de eerste fase wordt vluchtig gekeken naar relevantie van gegevens. Deze vluchtige eerste filtering van gegevens wordt direct en doorlopend uitgevoerd bij elke binnenkomst, waarbij irrelevante gegevens terstond worden verwijderd zodra is vastgesteld dat ze niet relevant zijn ('select while you collect'). De tweede fase, van stelselmatigheid, is gericht op het concrete onderzoek van de aldus gefilterde (en meer relevant en daarom hoogwaardiger geworden) gegevensverzameling. Met deze werkwijze wordt de inbreuk op de persoonlijke levenssfeer van personen die niet de aandacht van de diensten zouden moeten hebben, zo beperkt mogelijk gehouden omdat de inbreuk – door een snelle eerste fase – in de tijd beperkt is. Deze werkwijze sluit ook aan bij de jurisprudentie van het EHRM, die stelt dat data die niet relevant zijn voor het doel waarvoor ze zijn verkregen, onmiddellijk moeten worden vernietigd.¹⁰⁸

Uit het voorgestelde artikel 27, eerste lid, volgt dat gegevens verkregen door onderzoeksopdrachtgerichte interceptie zo spoedig mogelijk op hun relevantie worden onderzocht. Gegeven het feit dat, zoals hiervoor vermeld, de Europese rechters strenge eisen stellen aan de ongerichte verzameling van persoonsgegevens door de overheid (bulkinterceptie) is de wijze waarop aan artikel 27, eerste lid, in relatie tot de onderzoeksopdrachtgerichte interceptie uitvoering wordt gegeven, van cruciaal belang. Dit geldt met name voor de vraag op welk moment de bulk aan gegevens die in de eerste fase wordt geïntercepteerd, wordt gereduceerd tot die gegevens die voor verder onderzoek relevant kunnen zijn, hoe groot de hoeveelheid gegevens is die als onderdeel van de bulk aan een dergelijk selectieproces wordt onderworpen en hoe groot de hoeveelheid gegevens is die in 'de grote bak' ongeëvalueerde gegevens ten slotte achterblijft. De toelichting maakt dit onvoldoende duidelijk. Enerzijds stelt de toelichting dat het door Jacobs

¹⁰⁵Toelichting, paragraaf 3.3.4.4.7.4

¹⁰⁶Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX, TNO 2016 R10150, blz. 141.

¹⁰⁷Bart Jacobs, 'Select while you collect. Een bespreking van interceptie door inlichtingen- en veiligheidsdiensten', *NJB* 2016, blz. 256-261.

¹⁰⁸EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 255.

voorgestelde uitgangspunt ('select while you collect') 'op hoofdlijnen' recht wordt gedaan omdat aan de hand van (technische) filters irrelevante gegevens direct worden uitgefilterd en weggegooid. Anderzijds lijkt de benadering van Jacobs ook (deels) te worden afgewezen omdat de regering groot gewicht toekent aan het kunnen beschikken over 'achtergebleven' historische (meta)data door de diensten voor een periode van maximaal drie jaar.¹⁰⁹ Gegeven dit laatste moet niet worden uitgesloten dat er grote hoeveelheden gegevens die niet op relevantie zijn onderzocht, voor langere tijd opgeslagen blijven en derhalve geen recht wordt gedaan aan het door Jacobs verwoorde 'select while you collect' principe.

De Afdeling adviseert hierop in de toelichting, mede in het licht van de eerder genoemde Europese rechtspraak, nader in te gaan.

f. *Vernietiging niet onderzochte gegevens*

Artikel 47, vijfde lid, regelt dat gegevens die zijn verzameld in het kader van een onderzoeksopdrachtgerichte interceptie en die niet op relevantie zijn onderzocht na drie jaar worden vernietigd. Dit is een afwijking van de algemene regel uit artikel 27, dat voorschrijft dat niet onderzochte gegevens na een jaar worden vernietigd. De toelichting stelt dat het langer bewaren van de gegevens in de context van artikel 47 noodzakelijk is, omdat niet altijd op voorhand duidelijk is welke gegevens relevant zijn en historische metadata op een later moment nuttig kunnen zijn, bijvoorbeeld in het onderzoek nadat een aanslag heeft plaatsgevonden.¹¹⁰

De lengte van de bewaartermijnen is blijkens de eerder genoemde rechtspraak van het EHRM en het Hof van Justitie van de Europese Unie onderdeel van de toets naar de proportionaliteit van de inbreuk op het recht op bescherming van het privé-leven. In dat verband wijst de Afdeling in het bijzonder op het al genoemde arrest over de Dataretentierichtlijn. Aan de ongeldigverklaring van deze richtlijn wegens strijd met het recht op bescherming van het privé-leven en van persoonsgegevens lag onder meer ten grondslag dat de richtlijn ertoe verplichtte gegevens ongericht te verzamelen over alle burgers en een bewaringstermijn voorschreef van maximaal twee jaar zonder dat werd gepreciseerd dat de gekozen termijn noodzakelijk en proportioneel moet zijn.¹¹¹ De vraag of sprake is van een met het oog op artikel 8 EVRM te lange bewaartermijn moet daarom mede in het licht van de hoeveelheid gegevens die ongericht zijn verzameld, worden beantwoord.

Zoals hiervoor aangegeven (zie onderdeel e) bevatten noch het wetsvoorstel noch de toelichting een duidelijke indicatie van de omvang van de gegevens die op grond van een onderzoeksgerichte interceptie kunnen worden verzameld en hoeveel van deze gegevens kort nadat zij zijn verzameld op relevantie zullen worden onderzocht. Om die reden kan niet worden uitgesloten dat er grote hoeveelheden gegevens die niet op relevantie zijn onderzocht en die betrekking kunnen hebben op grote aantallen burgers, voor langere tijd zullen zijn opgeslagen. Dat geldt te meer nu de diensten in bepaalde gevallen afhankelijk zullen zijn van de

¹⁰⁹Toelichting, paragraaf 12.2.

¹¹⁰Toelichting, 3.3.2.3 Het onderzoek op relevantie van gegevens en de vernietiging van gegevens.

¹¹¹HvJ EU 8 april 2014, Digital Rights Ireland, C293/12 en C-594/12.

wijze waarop het dataverkeer kan worden verzameld voor de begrenzing van de gegevens die zij daadwerkelijk binnenkrijgen.¹¹² De bewaartermijn moet ten slotte worden gezien in het licht van het feit dat deze gegevens op grond van het wetsvoorstel gedurende de gehele drie jaar aan anderen kunnen worden verstrekt, waaronder aan buitenlandse diensten (zie ook punt i), die zelf niet in alle gevallen gebonden zijn aan een maximale bewaartermijn.¹¹³

De Afdeling begrijpt dat, zoals de toelichting stelt, de bewaartermijn van drie jaar samenhangt met de notie dat een integraal onderdeel van het inlichtingenproces wordt gevormd door de analyse van historische data.¹¹⁴ Het recht op bescherming van het privé-leven zoals neergelegd in onder meer artikel 8 EVRM stelt evenwel grenzen aan de termijn gedurende welke zulke gegevens mogen worden bewaard. In de toelichting wordt onvoldoende gemotiveerd waarom een termijn van drie jaar in dit geval noodzakelijk en proportioneel is in een democratische samenleving als bedoeld in artikel 8, tweede lid, EVRM.¹¹⁵ Gelet op de eerder genoemde rechtspraak en gelet op de hiervoor genoemde omstandigheden acht de Afdeling de kans klein dat het EHRM in het kader van artikel 8, tweede lid, EVRM een termijn van drie jaar voor het bewaren van niet onderzochte 'bulkgegevens' aanvaardbaar acht. Daarnaast wijst het EHRM op het belang van het direct vernietigen van data die niet relevant zijn met betrekking tot het doel in het kader waarvan zij verkregen zijn.¹¹⁶ Weliswaar bevat het wetsvoorstel daarover regels¹¹⁷ maar deze specificeren niet binnen welke termijn niet relevante gegevens moeten worden vernietigd.

De Afdeling adviseert tot een substantiële verkorting van de bewaartermijn in artikel 47, vijfde lid, en het wetsvoorstel daartoe aan te passen.

g. *Vernietiging niet relevante gegevens*

Artikel 47, vijfde lid, ziet op de vernietiging van niet relevante gegevens die in het kader van een onderzoekso opdrachtgerichte interceptie van kabelgebonden verkeer zijn verkregen. Het artikel lijkt, ook gelet op de toelichting, te impliceren dat gegevens die onderzocht zijn en binnen die onderzoekso opdracht niet relevant zijn moeten worden vernietigd.

Artikel 27, eerste lid, kent echter een algemene regeling van de vernietiging van gegevens, die ook van toepassing is op gegevens die in het kader van een onderzoekso opdrachtgerichte interceptie zijn verzameld. Dit eerste lid bepaalt onder meer dat gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het

¹¹² Bijvoorbeeld in het geval een onderzoekso opdracht gerichte interceptie zich uitstrekt tot het netwerk van de NS of het verkeer via WhatsApp, is niet duidelijk of al geselecteerd kan worden bij de aanbieder van deze dienst, of dat de selectie bij de diensten zelf zal moeten plaatsvinden.

¹¹³ Zie toelichting, bijlage 5 Schematisch overzicht wetgeving van enkele andere landen.

¹¹⁴ Toelichting, paragraaf 3.3.4.4.7.4.

¹¹⁵ De bewaartermijn van drie jaar wordt in de toelichting ook slechts summier getoetst aan artikel 8 EVRM en de daarop gebaseerde rechtspraak van het EHRM. Zie paragraaf 9.2.1.

¹¹⁶ EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 255.

¹¹⁷ Artikel 20, eerste en derde lid, van het voorstel. Zie ook artikel 27, eerste lid, en 47, vijfde lid, van het voorstel.

onderzoek *dan wel enig ander lopend onderzoek* vallend onder de taken, bedoeld in artikel 8, tweede lid, onder a en d, en artikel 10, tweede lid, onder a, c en e, worden vernietigd. Er kan dus sprake zijn van relevantie in relatie tot het onderzoek waarin de gegevens zijn verworven maar ook in relatie tot enig ander lopend onderzoek. Dit zou betekenen dat gegevens die verzameld zijn in een onderzoeksoopdrachtgerichte onderzoek bewaard mogen blijven als zij relevant kunnen zijn voor een ander lopend onderzoek van de diensten.

De toelichting gaat niet in op de verhouding tussen artikel 27, eerste lid en artikel 47, vijfde lid. Gelet op de zeer ruime taakomschrijvingen in de genoemde artikelen, roept dit de vraag op of vernietiging van onderzochte maar niet relevant geachte gegevens hiermee in de praktijk niet eerder uitzondering zal zijn dan regel. De Afdeling acht dat problematisch. Daar – zoals de toelichting ook onderkent ¹¹⁸ – vernietiging van gegevens een belangrijke waarborg is tegen een te grote inbreuk op het recht op bescherming van het privé-leven, moet de regeling die daarop ziet zo specifiek mogelijk zijn opdat, mede gelet op artikel 8 EVRM, gegarandeerd wordt dat gegevens niet langer bewaard worden dan strikt noodzakelijk is.

De Afdeling adviseert in de toelichting nader in te gaan op de vernietiging van niet relevante gegevens en in het bijzonder op de verhouding tussen artikel 27, eerste lid, en artikel 47, vijfde lid, en zo nodig het voorstel aan te passen.

h. *Vernietiging versleutelde gegevens*

Artikel 47, zesde lid, ziet op de bewaartermijn van versleutelde gegevens die door de diensten verzameld zijn. Ook hier geldt een bewaartermijn van drie jaar, maar deze termijn begint pas te lopen op het moment dat de versleuteling ongedaan is gemaakt. Het voorstel bevat geen bepalingen die zien op de termijn waarbinnen ontsleuteling moet plaatsvinden. Dat betekent dat de gegevens in versleutelde vorm in theorie voor altijd bewaard zouden kunnen worden. Daarnaast lijkt het voorstel de mogelijkheid te bieden deze versleutelde gegevens aan derden te verstrekken, waaronder buitenlandse diensten (zie ook punt i).

In het licht van de bescherming van de persoonlijke levenssfeer en het belang van duidelijk afgebakende bewaartermijnen acht de Afdeling bovengenoemde regeling ontoereikend. Zij acht het noodzakelijk dat in het voorstel wordt geregeld op welke termijn versleutelde gegevens ontsleuteld moeten worden, dan wel de bijzondere regeling voor versleutelde gegevens te schrappen en aan te sluiten bij de reguliere bewaartermijnen voor gegevens.

De Afdeling adviseert het voorstel aan te passen.

i. *Samenwerking buitenland*

Het voorstel bevat in paragraaf 6.2 bepalingen over samenwerking met diensten van andere landen. In artikel 86, derde lid, wordt een aantal criteria genoemd dat

¹¹⁸Toelichting, 9.2.1 Toetskader artikel 8 EVRM, Voorzienbaarheid: eisen aan de verwerking van gegevens en 9.4, Interceptie van de inhoud van communicatie.

moet worden betrokken bij de keuze om te gaan samenwerken met een andere dienst. Het gaat hierbij onder meer om de democratische inbedding van die dienst en de eerbiediging van de mensenrechten. Artikel 87, tweede lid, ziet op de verstrekking van niet geëvalueerde gegevens aan een dienst waarmee een samenwerkingsrelatie is aangegaan. Uit deze artikelen volgt dat voordat aan een buitenlandse dienst ongeëvalueerde gegevens worden verstrekt, een 'wegingsnotitie' wordt opgesteld waarbij de genoemde criteria worden betrokken. Dit zou moeten waarborgen dat slechts in uitzonderlijke gevallen gegevens worden verstrekt aan landen die niet aan deze criteria voldoen.

Artikel 61, eerste lid, onder d, juncto derde lid, van het voorstel kent echter ook een regeling voor de mededeling over niet geëvalueerde gegevens aan buitenlandse diensten. In tegenstelling tot de artikelen 86 en 87 wordt hierbij niet de eis gesteld dat het gaat om diensten waarmee een samenwerkingsrelatie is aangegaan. Hierdoor is onduidelijk of de toets aan de criteria van artikel 86, derde lid ook in het kader van de toepassing van artikel 61, eerste lid, onder d, juncto derde lid moet worden uitgevoerd. Daarnaast is niet duidelijk waarom het voorstel twee regelingen voor deze overdracht bevat en waarom deze verschillend is geformuleerd.

De overdracht van niet geëvalueerde gegevens, met name die gegevens die zijn verkregen uit grootschalige interceptie, vormt een ernstige inbreuk op het recht op bescherming van de persoonlijke levenssfeer van burgers.¹¹⁹ Dit geldt *a fortiori* indien deze gegevens worden overgedragen aan buitenlandse diensten, omdat daarmee effectieve controle van de Nederlandse toezichthouder op het gebruik van die gegevens ontbreekt. Ook kennen sommige landen een veel langere bewaartermijn dan in het voorstel is opgenomen. Om die reden dient deze overdracht met voldoende waarborgen omkleed te zijn. Dit betekent dat in alle gevallen een toetsing aan de criteria van artikel 86, derde lid, noodzakelijk is voordat gegevens kunnen worden overgedragen. Daarbij zou expliciet bepaald moeten worden dat overdracht aan landen die niet voldoen aan de genoemde criteria alleen in uitzonderlijke gevallen kan plaatsvinden.¹²⁰

De Afdeling adviseert op grond van het bovenstaande de regeling met betrekking tot overdracht van gegevens aan buitenlandse diensten uitsluitend te regelen in paragraaf 6.2.

j. *Profilering en geautomatiseerde besluitvorming*

In artikel 59, eerste lid, wordt de bevoegdheid van de diensten geregeld om een geautomatiseerde data-analyse toe te passen met betrekking tot uit diverse bronnen verkregen gegevens. In het tweede lid worden drie vormen van geautomatiseerde data-analyse genoemd die in elk geval onder de in het eerste lid genoemde bevoegdheid vallen. Het betreft de geautomatiseerde vergelijking van

¹¹⁹ 'Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten', Universiteit Leiden, blz. 28.

¹²⁰ Rapport van de CTIVD nr. 49 over de uitwisseling van ongeëvalueerde gegevens door de AIVD en de MIVD.

gegevens of bestanden (onderdeel a), het doorzoeken van gegevens of bestanden aan de hand van profielen (onderdeel b) en de vergelijking van gegevens of bestanden met het oog op het opsporen van bepaalde patronen (onderdeel c). Met betrekking tot een van deze vormen, het doorzoeken aan de hand van profielen (onderdeel b), wordt in het derde lid bepaald dat het bevorderen of treffen van maatregelen jegens een persoon uitsluitend op basis van de resultaten van een zodanige doorzoeking, niet is toegestaan. Met 'profielen' wordt blijkens de toelichting met name bedoeld op 'een samenstel van kenmerken met betrekking tot bijvoorbeeld een bepaalde categorie van onderzoekssubjecten, die uit analyse van eigen onderzoeken, onderzoeken van derden of ervaringsgegevens naar voren zijn gekomen'.¹²¹

Het in artikel 59, derde lid, neergelegde verbod sluit aan bij bestaande¹²² en toekomstige¹²³ Europese regelgeving. Het achterliggende uitgangspunt is, dat beslissingen of maatregelen jegens personen niet mogen worden genomen zonder menselijke tussenkomst: de computer mag de mens niet of althans niet volledig vervangen. Deze gedachte hangt samen met de constatering van de WRR in het eerder genoemde rapport, dat Big Data-analyses een gefragmenteerd, eenzijdig en onjuist beeld kunnen geven van de werkelijkheid. Daardoor kunnen gemakkelijk fouten optreden. Als bijvoorbeeld een door Big Data-analyses gevonden correlatie zonder meer voor een causaal verband wordt aangezien, kunnen al snel verkeerde conclusies worden getrokken. Daarom vergen Big Data-analyses vrijwel standaard nader onderzoek, analyse en menselijke afweging.¹²⁴

In het licht van het voorgaande rijst de vraag of het voorgestelde verbod van artikel 59, derde lid, niet te beperkt is. Zoals uit het voorgaande bleek is profilering slechts een van de vormen van geautomatiseerde data-analyse. De vraag is daarom of het genoemde verbod, ook in relatie tot de bevoegdheid tot onderzoeksopdrachtgerichte interceptie¹²⁵, niet moet worden verbreed tot alle vormen van geautomatiseerde data-analyse. De algemene, in artikel 18, derde lid, neergelegde zorgplicht¹²⁶ met betrekking tot de betrouwbaarheid van de door de diensten verwerkte gegevens, is met het oog daarop onvoldoende specifiek. De hiervoor bedoelde verbreding sluit aan bij artikel 22 van Verordening (EU) 2016/679. Hierin wordt geregeld dat een persoon niet mag worden onderworpen aan 'een uitsluitend op geautomatiseerde verwerking, waaronder profilering', gebaseerd besluit. Deze bepaling heeft daarmee derhalve een ruimere reikwijdte dan alleen profilering.

¹²¹ Toelichting, paragraaf 3.5.

¹²² Artikel 15 Richtlijn 95/46/EG.

¹²³ Artikel 22 Verordening (EU) 2016/679 (Algemene verordening gegevensbescherming). Deze verordening zal in 2018 Richtlijn 95/46/EG vervangen.

¹²⁴ WRR 2016, blz. 132-133.

¹²⁵ Zie artikel 49, eerste lid, onder b, van het voorstel.

¹²⁶ Artikel 18, derde lid, van het voorstel luidt: De gegevens die in het kader van de taakuitvoering van de diensten worden verwerkt, zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend.

De Afdeling adviseert in de toelichting op het bovenstaande in te gaan en zo nodig het wetsvoorstel aan te passen.

k. *Aanpassing technische systemen*

In de PIA wordt aanbevolen om in het wetsvoorstel een bepaling op te nemen die waarborgt dat gegevensbescherming in het technische ontwerp van systemen wordt ingebouwd. Daarbij gaat het er enerzijds om dat instellingen in systemen standaard op de meest privacy-vriendelijke manier worden ingericht, zodat gebruikers niet extra moeite moeten doen om gegevens beter te beschermen (gegevensbescherming *by design*) en anderzijds dat de systemen die de verwerking mogelijk maken zo moeten zijn ontworpen en ingericht dat zo min mogelijk persoonsgegevens worden verwerkt (gegevensbescherming *by default*).¹²⁷ De regering heeft deze aanbeveling niet overgenomen. Naar het oordeel van de regering kan een dergelijke bepaling aangewezen zijn indien de verantwoordelijke voor de gegevensverwerking zelf veel ruimte is gelaten om met het oog op diens taak de wijze waarop hij gegevens verwerkt, invulling te geven en daarbij de in geding zijnde privacy-risico's te minimaliseren. Dat geval zou zich hier, gelet op het in het wetsvoorstel neergelegde specifieke kader, niet voordoen. Daarom kan volgens de regering worden volstaan met een bepaling waarin de hoofden van dienst de plicht opgelegd krijgen om ervoor te zorgen dat de technische, personele en organisatorische maatregelen in verband met de verwerking van gegevens in overeenstemming zijn met hetgeen bij of krachtens de wet is bepaald (artikel 24, eerste lid).¹²⁸

Kenmerk van Big Data-toepassingen is dat grote hoeveelheden data met behulp van geavanceerde technieken op geautomatiseerde wijze worden geselecteerd, verwerkt en geanalyseerd. In die constellatie is het van steeds groter belang geworden dat reeds bij het ontwerpen en inrichten van de technische systemen die de Big Data-analyses moeten uitvoeren, rekening wordt gehouden met wettelijke eisen van noodzakelijkheid, doelbinding en non-discriminatie. Omdat technische systemen meestal meer kunnen dan is toegestaan, is van cruciaal belang dat gedurende de ontwerpfase wordt bepaald of en zo ja, hoe het systeem zo kan worden ingericht dat bepaalde gegevensverwerkingen technisch moeilijk zijn uit te voeren of onmogelijk worden gemaakt.¹²⁹ Om het belang hiervan te onderstrepen is in de Algemene verordening gegevensbescherming – naast de algemene beveiligingsverplichting – een specifieke verplichting opgenomen om – kort gezegd – passende technische en organisatorische maatregelen te nemen die erop gericht zijn de beginselen van gegevensbescherming bij het ontwerpen van systemen in te bouwen.¹³⁰

In het licht van het voorgaande acht de Afdeling de afwijzing van de genoemde aanbeveling zoals in de toelichting verwoord niet overtuigend. In de eerste plaats bevat het wetsvoorstel weliswaar een specifieke regeling van bevoegdheden, maar

¹²⁷ PIA, blz. 158. Zie voor een nadere onderbouwing blz. 148 e.v.

¹²⁸ Toelichting, paragrafen 12.3.2.3 en 3.2.6

¹²⁹ M. Hildebrandt, Data-Gestuurde Intelligentie in het strafrecht, Preadvies NJV 2016, blz. 214 e.v.

¹³⁰ Artikel 25 Verordening (EU) 2016/679.

het globale kader van uitgangspunten¹³¹ dat de beleidsruimte van de diensten bepaalt is zeer ruim. In die zin zou, ook volgens het door de regering geformuleerde criterium, aanleiding bestaan om een bepaling zoals aanbevolen in het wetsvoorstel op te nemen. Voorts is de reeds in het wetsvoorstel opgenomen zorgplicht te algemeen en biedt deze daardoor te weinig houvast om in concrete zin te waarborgen dat bij het ontwerpen van technische systemen met de beginselen van gegevensbescherming rekening wordt gehouden. In de toelichting op het artikel dat die zorgplicht voor de hoofden van dienst regelt wordt ook in het geheel niet ingegaan op de wijze waarop met het oog op het bovenstaande de zorgplicht zou moeten worden uitgevoerd.

De Afdeling adviseert om in de toelichting op het bovenstaande in te gaan en het wetsvoorstel zo nodig aan te passen.

5. Conclusie: verenigbaarheid met het EVRM

De belangrijkste conclusies omtrent de verenigbaarheid van het wetsvoorstel met het EVRM, gebaseerd op de voorgaande beschouwingen in de paragrafen 2-4, zijn de volgende.

Het wetsvoorstel bevat met het oog op de naleving van het EVRM een aanzienlijk aantal belangrijke waarborgen (punt 2). Daarmee wordt voldaan aan een groot aantal essentiële vereisten die door het EHRM met name met het oog op artikel 8 EVRM gesteld worden. De Afdeling acht het voorstel op het punt van de vereiste deugdelijke wettelijke basis, in het licht van de kenbaarheid en voorzienbaarheid, adequaat. De uitbreiding van bevoegdheden, waaronder de bevoegdheid tot ongerichte interceptie van kabelgebonden communicatie acht de Afdeling op zichzelf legitiem; de noodzaak daarvan acht zij in het licht van artikel 8, tweede lid, EVRM voldoende aangetoond. De wet bevat voorts een stelsel van waarborgen met het oog op de beginselen van proportionaliteit en subsidiariteit, alsmede criteria met betrekking tot de opslag en vernietiging van gegevens.

De Afdeling heeft echter ernstige twijfels over de *daadwerkelijke effectiviteit* van het voorgestelde stelsel van toezicht (punt 3). Daartoe benadrukt zij, dat de verplichting om te voorzien in een effectief stelsel van toezicht primair op de verdragsstaat rust, niet op het – van een afstand oordelende – Hof in Straatsburg. Het gaat er dan ook niet uitsluitend om dat een toezichtstelsel formeel – op papier – voldoet aan de criteria die het EHRM stelt, zodat het in ‘Straatsburg’ *EVRM-proof* is. Het gaat er vooral om, dat het stelsel van toezicht is toegesneden op de specifieke inrichting van het nationale systeem, en daarbinnen in samenhang bezien daadwerkelijk effectieve bescherming biedt. Het wetsvoorstel schiet op dit punt tekort; de Afdeling adviseert de TIB in het voorstel te schrappen en het toezicht – met uitzondering van de behandeling van klachten – bij de CTIVD te concentreren.

¹³¹ Zie met name paragraaf 3.1 Algemene bepalingen ter zake van de verwerking van persoonsgegevens (artikelen 17-24 van het voorstel).

Daarnaast is de Afdeling met betrekking tot de proportionaliteit van met name de grootschalige gegevensverzameling (Big Data) er voorshands niet van overtuigd dat het voorstel en de motivering in de memorie van toelichting op alle punten daadwerkelijk voldoet aan de vereisten die voortvloeien uit het EVRM (punt 4). In het bijzonder heeft de Afdeling ernstige twijfels over de verenigbaarheid met het EVRM als het gaat om de bewaartermijn van drie jaar als bedoeld in artikel 47, vijfde lid. Op het laatste punt adviseert zij om in het wetsvoorstel een substantieel kortere bewaartermijn op te nemen.

6. Strafrechtelijke handhaving medewerkingsplicht

Aan de Afdeling is ook verzocht om in haar advies in te gaan op het in het wetsvoorstel neergelegde stelsel van handhaving met betrekking tot de daarin voorziene medewerkings- en informatieplichten.¹³² De voorgestelde bepaling voorziet, overeenkomstig de huidige Wet op de inlichtingen- en veiligheidsdiensten 2002, in een stelsel van strafrechtelijke handhaving. Aan de Afdeling is gevraagd of dit een passend stelsel is of dat een stelsel van bestuursrechtelijke handhaving meer in de rede ligt.

De Afdeling merkt op dat de toelichting, noch de onderliggende stukken ingaan op de voor- en nadelen van beide stelsels en de reden waarom in het voorliggend voorstel wordt gekozen voor strafrechtelijke handhaving. Ook in de consultatiereacties wordt geen aandacht besteed aan dit onderwerp. Daarnaast blijkt ook niet uit de toelichting of de onderliggende stukken dat er een probleem zou zijn met het huidige stelsel van strafrechtelijke handhaving. Daarmee geeft de regering zelf geen argumenten waarom van het strafrechtelijke stelsel van handhaving afgestapt zou moeten worden. De Afdeling ziet ook overigens geen aanleiding om over te gaan naar een stelsel van bestuursrechtelijke handhaving. Derhalve ziet de Afdeling geen reden voor een wijziging van de bestaande regeling in het wetsvoorstel.

7. Vormgeving TIB

Onverminderd hetgeen de Afdeling in punt 3 over de TIB heeft opgemerkt, maakt zij over de vormgeving van de TIB – als deze ingevoerd zou worden – de volgende opmerkingen.

a. *Enkelvoudige of meervoudige samenstelling*

Het valt de Afdeling op dat in het voorstel en de toelichting weliswaar gesproken wordt over de commissie, maar dat de beoordeling per geval gedaan zal worden door één enkel lid van deze commissie.¹³³ De toelichting motiveert die keuze niet. Gegeven het grote belang dat de toelichting toekent aan toetsing vooraf van de inzet van deze bevoegdheden zou het voor de hand liggen om te bepalen dat deze

¹³² Artikel 141 van het voorstel.

¹³³ Artikel 35, derde lid, van het voorstel.

toetsing plaatsvindt door de gehele commissie. Voor spoedgevallen zou een uitzondering mogelijk gemaakt kunnen worden. Het wetsvoorstel zou in deze zin aangepast moeten worden.

b. *Benodigde deskundigheid*

De TIB toetst de last die de diensten hebben opgesteld en waarvoor de minister reeds toestemming heeft gegeven. Het gaat hierbij met name om een rechtmatigheidstoets.¹³⁴ Leden van de TIB dienen te beschikken over rechterlijke ervaring. De Afdeling wijst erop dat het met name voor het beoordelen van de noodzaak en proportionaliteit van de inzet van grootschalige interceptie van belang is dat de TIB ook over voldoende technische deskundigheid en inzicht in veiligheidsrisico's beschikt. In het voorstel, noch in de toelichting wordt aangegeven hoe hierin wordt voorzien.

c. *Verantwoording*

Gegeven de eerdere discussies over openbaarheid van bijvoorbeeld het aantal gevallen waarin een bevoegdheid wordt ingezet is het van belang dat duidelijk is welke informatie vanuit de toezichthouders openbaar wordt gemaakt. In het voorstel zijn geen bepalingen opgenomen over de wijze waarop de TIB verantwoording aflegt over haar werkzaamheden. Dit lijkt te impliceren dat een dergelijke verantwoording niet zal plaatsvinden. In dat geval kan niet worden nagegaan of, en zo ja onder welke omstandigheden, de TIB een door de minister gegeven toestemming onrechtmatig heeft geacht. Daarmee rijst de vraag of de beoogde waarborg van een onafhankelijke toetsing vooraf op voldoende wijze wordt ingevuld. Om die reden zou het wetsvoorstel moeten voorzien in een afdoende regeling omtrent de verantwoording die de TIB aflegt.

d. *Conclusie*

Indien besloten wordt de TIB in te voeren adviseert de Afdeling het voorstel en toelichting in het licht van het bovenstaande aan te passen en aan te vullen.

8. Mandaat

Artikel 29 voorziet in een algemene regeling met betrekking tot mandaatverlening voor het geven van toestemmingen voor het inzetten van bijzondere bevoegdheden. Dit artikel maakt ruime mandaatverlening mogelijk. Het artikel bepaalt ook dat in de artikelen die zien op specifieke bijzondere bevoegdheden afwijkende bepalingen kunnen worden opgenomen over mandaat. Bij de meeste bijzondere bevoegdheden gebeurt dit ook. Dit leidt ertoe dat een onoverzichtelijk beeld ontstaat waar het gaat om mandaatverlening. Tevens rijst de vraag wat het nut is van een algemene regeling indien daar in een groot aantal gevallen van wordt afgeweken. In dat geval is het duidelijker indien elke bepaling waarin een toestemmingsvereiste is opgenomen zijn eigen regeling over mandaat bevat.

¹³⁴Toelichting, paragraaf 9.2.1 Toetskader artikel 8 EVRM, *Voorzienbaarheid: de toestemmingssystematiek*.

De Afdeling adviseert het voorstel op dit punt aan te passen.

9. Binnendringen via een geautomatiseerd werk van een derde

In het voorgestelde artikel 44, eerste lid, onder b, wordt expliciet de bevoegdheid toegekend aan de diensten om via een geautomatiseerd werk van een derde binnen te dringen in een geautomatiseerd werk van een 'doelwit' (target). Op deze bevoegdheid is in de consultatiereacties kritisch gereageerd, onder meer omdat de inzet van deze bevoegdheid voor een derde niet voorzienbaar en disproportioneel zou zijn. Ook is deze bevoegdheid niet met meer waarborgen omgeven dan bij toepassing van de bevoegdheid jegens degene die feitelijk het doelwit van de operatie is. Daarnaast is volgens de genoemde reacties onduidelijk hoe de derde wordt beschermd tegen de risico's en mogelijke gevolgen van het binnendringen in een aan hem toebehorend geautomatiseerd werk. Tevens wijzen verschillende instanties erop dat het binnendringen via derden gevolgen heeft voor de integriteit en betrouwbaarheid van het internet en de daarop aangesloten ICT-systemen. Het gebruik van malware en het exploiteren van in geautomatiseerde werken onderkende zwakheden kan volgens hen vergaande gevolgen hebben, die niet op voorhand zijn te voorzien en te controleren.¹³⁵

In reactie op deze opmerkingen is in de toelichting nader gemotiveerd waarom deze bevoegdheid essentieel is voor de diensten. Daarbij valt het de Afdeling op dat de toelichting niet geheel eenduidig is over de vraag wanneer deze bevoegdheid zal worden ingezet. Zo wordt enerzijds gesteld: "Belangrijk is te beseffen dat binnendringen via een geautomatiseerd werk van een derde een ultimatum remedium is. De diensten zullen altijd eerst proberen rechtstreeks binnen te dringen in het geautomatiseerde werk van het target zelf."¹³⁶

Daar staat tegenover dat de toelichting ook stelt: "De technische realiteit leert dat targets over het algemeen veiligheidsbewust zijn, maar dat zich operationele kansen tot het benutten van zwakheden kunnen voordoen bij technische randgebruikers, zoals medehuurders van een bepaalde server, welke kunnen leiden tot het succesvol binnendringen van het geautomatiseerde werk van het target."¹³⁷ Vervolgens wordt aangegeven dat de diensten zich in de praktijk al in het overgrote deel van de gevallen toegang tot het geautomatiseerd werk van een 'target' verschaffen via het geautomatiseerd werk van een derde.¹³⁸

Daarnaast wijst de Afdeling erop dat in het voorstel noch de toelichting een nadere duiding wordt gegeven van het begrip 'derde'. De toelichting heeft het met name over providers, tussenleveranciers en dienstverleners. Voor deze organisaties kent het voorstel echter in een aantal bepalingen al de verplichting om mee te werken aan het verkrijgen van toegang tot het geautomatiseerde werk van het doelwit.¹³⁹

¹³⁵ Toelichting, paragraaf 12.2.4

¹³⁶ Toelichting, paragraaf 3.3.4.4.6.

¹³⁷ Toelichting, paragraaf 3.3.4.4.6.

¹³⁸ Toelichting, paragraaf 3.3.4.4.6.

¹³⁹ Zie onder meer de artikelen 44, negende lid, 53 en 54 van het voorstel.

Als niet is beoogd om de bevoegdheid om binnen te dringen via een derde ook toe te passen op andere categorieën dan aangegeven in de toelichting, zou dit in het voorstel dan wel in de toelichting verduidelijkt moeten worden. Indien dit wel is beoogd zou dit duidelijker moeten blijken uit de toelichting en dient daarbij tevens te worden ingegaan op de vraag of en in welke gevallen het binnendringen via het werk van een derde, in het algemeen een individuele burger, geoorloofd is.

Ten slotte wijst de Afdeling erop dat de bijschrijfbevoegdheid uit het achtste lid van artikel 44 ook van toepassing is op het binnendringen via een derde. Dit betekent dat weliswaar voor het eerste geautomatiseerde werk van de derde de verzwaarde procedure met toestemming van de minister geldt, maar dat deze toestemming niet hoeft te worden verkregen voor andere geautomatiseerde werken die deze derde gebruikt. Gelet op de hierboven genoemde nadelen die kleven aan het binnendringen via het werk van een derde acht de Afdeling het noodzakelijk dat voor ieder werk dat hiervoor gebruikt gaat worden de afweging van de technische risico's, bedoeld in het vierde lid van artikel 44, wordt gemaakt. Dit betekent dat voor derden per geautomatiseerd werk dat door hen wordt gebruikt, toestemming zou moeten worden gevraagd.

De Afdeling adviseert in de toelichting op het bovenstaande in te gaan en zo nodig het voorstel aan te passen.

10. Toelichting

De Afdeling merkt op dat de toelichting omvangrijk is en de verdeling tussen het algemeen deel en de artikelsgewijze toelichting onevenwichtig is. Het grootste deel van het algemeen deel van de toelichting is feitelijk een bespreking van de verschillende artikelen en zou daarom moeten worden overgeheveld naar de artikelsgewijze toelichting. Dit maakt het eenvoudiger om per artikel de daarbij behorende toelichting te vinden. Het algemeen deel zou zich met name moeten richten op een bespreking van nut en noodzaak, de afweging tussen de functie van de diensten en de grondrechten van burgers en de inrichting van het toezicht. Een dergelijke opzet maakt het ook bij eventuele toekomstige wijzigingen van het voorstel eenvoudiger om te bezien waarom een bepaald artikel is opgenomen en op de betreffende manier is verwoord. Daarnaast zou moeten worden bezien of de toelichting bondiger kan worden geformuleerd.

De Afdeling adviseert de verdeling van onderwerpen tussen het algemeen deel van de toelichting en het artikelsgewijs deel te bezien en tevens te bezien of de toelichting bondiger kan worden geformuleerd.

11. Overige opmerkingen

a. *Samenhang met het wetsvoorstel bronbescherming in strafzaken*

In het wetsvoorstel bronbescherming in strafzaken, dat op dit moment aanhangig is bij de Tweede Kamer, is bij nota van wijziging toegevoegd dat de vordering van communicatiegegevens van journalisten slechts kan worden verkregen na

machtiging door de rechter-commissaris.¹⁴⁰ Dit toestemmingsvereiste strekt zich uit tot alle communicatie van journalisten en is daarmee ruimer dan het voorliggende wetsvoorstel, waarin slechts machtiging van de rechtbank nodig is als de uitoefening van de bijzondere bevoegdheden "is gericht op het achterhalen van de bron van de journalist".¹⁴¹

De Afdeling merkt op dat door de uitbreiding van de bronbescherming van journalisten in het strafrecht een verschil ontstaat met de bronbescherming in de Wiv, waarvoor onvoldoende motivering bestaat. Daar komt bij dat de voorgestelde toets op de verwerving van communicatie van advocaten ook ruimer is dan die voor journalisten.¹⁴²

De Afdeling adviseert, gelet op de ontwikkelingen in de bronbescherming in het strafrecht, het toestemmingsvereiste voor de uitoefening van bijzondere bevoegdheden jegens een journalist te laten aansluiten bij de formulering van het voorgestelde artikel 29, zesde lid, en het toestemmingsvereiste voor te schrijven voor alle gevallen waarbij de uitoefening van de bevoegdheden kan leiden tot het achterhalen van de bron van de journalist.

b. Medewerkingsplicht oud-medewerkers

Artikel 105, eerste lid, verplicht een ieder die betrokken is bij de uitvoering van de Wiv desgevraagd aan CTIVD alle noodzakelijke inlichtingen te verstrekken en medewerking te verlenen. In haar advies over de consultatieversie heeft de CTIVD geadviseerd de ontheffing van de geheimhoudingsplicht ook te laten gelden voor oud-medewerkers van de diensten. Op grond van het voorgestelde artikel 134, derde lid, mogen zij alleen een verklaring afleggen aan de CTIVD over staatsgeheime zaken als zij door de betrokken minister(s) ontheven zijn van hun geheimhoudingsplicht.

De Afdeling onderschrijft het standpunt van de CTIVD dat het voor het functioneren van het toezicht cruciaal is dat (oud-)medewerkers van de diensten hun geheimhoudingsplicht niet kunnen inroepen tegenover de CTIVD. De regering heeft het advies van de CTIVD op dit punt echter niet overgenomen, zonder dat te motiveren.

De Afdeling adviseert alsnog te voorzien in een medewerkingsplicht aan de CTIVD voor oud-medewerkers van de diensten.

c. "Mededeling" of "verstrekken"

Het wetsvoorstel maakt op verschillende plaatsen onderscheid tussen enerzijds het verstrekken van gegevens en anderzijds het doen van mededeling omtrent door de diensten verwerkte gegevens. In het voorgestelde artikel 61 wordt bijvoorbeeld

¹⁴⁰ Kamerstukken II 2014/15, 34 032, nr. 9.

¹⁴¹ Artikel 29, vijfde lid, van het voorstel. Dit artikel is overigens gelijklopend aan het voorstel tot wijziging van de Wiv 2002 in verband met de bronbescherming van journalisten, zoals dat nu in behandeling is bij de Tweede Kamer (Kamerstukken II 2014/15, 34 027, nr. 2).

¹⁴² Artikel 29, zesde lid, van het voorstel.

geregeld dat de diensten over de verwerking van gegevens mededeling kunnen doen aan externe personen of organisaties. Met de term "mededeling" lijkt in dat artikel echter "verstrekking" bedoeld te worden. De bepaling staat in de paragraaf "De externe verstrekking van gegevens" en artikel 63 gebruikt ook de term verstrekking.¹⁴³ Het doen van mededeling over ongeëvalueerde gegevens, zoals bedoeld in artikel 61, derde lid, is overigens ook weinig zinvol indien die gegevens niet tevens worden verstrekt, dan wel daarin inzage wordt verleend. De inhoud van de ongeëvalueerde gegevens is immers onbekend, dus een mededeling daarover zal weinig inhoudelijk kunnen zijn.

Uit de tekst van het voorgestelde artikel 67, blijkt dat ook een inhoudelijk verschil is beoogd tussen verstrekking van persoonsgegevens en mededeling daarover. Geregeld is dat verouderde gegevens weliswaar niet meer mogen worden verstrekt, maar dat daarover aan bepaalde instanties wel "slechts" mededeling kan worden gedaan.¹⁴⁴

De Afdeling adviseert in het wetsvoorstel nauwkeuriger gebruik te maken van de termen "verstrekking" en "mededeling" en deze begrippen ook in de toelichting consistent te gebruiken.

12. Conclusie en dictum

De Afdeling concludeert dat het wetsvoorstel een aanzienlijk aantal belangrijke waarborgen bevat waarmee voldaan wordt aan enkele essentiële vereisten van het EVRM. De Afdeling is echter met betrekking tot de proportionaliteit van met name de grootschalige gegevensverzameling (Big Data) er niet van overtuigd dat het voorstel en de motivering in de memorie van toelichting op alle punten daadwerkelijk voldoen aan de vereisten die voortvloeien uit het EVRM.

De Afdeling acht bovendien het voorgestelde stelsel van toezicht als geheel niet toereikend. Zij heeft ernstige twijfels over de daadwerkelijke effectiviteit van dat stelsel. Deze effectiviteit van het toezicht is van wezenlijk belang voor de werking van de voorgestelde nieuwe Wet op de inlichtingen- en veiligheidsdiensten.

De Afdeling advisering van de Raad van State heeft blijkens het vorenstaande bezwaar tegen de inhoud en opzet van het voorgestelde stelsel van toezicht en geeft U in overweging dit voorstel van wet op dit punt niet aldus te zenden aan de Tweede Kamer der Staten-Generaal.

De vice-president van de Raad van State,



¹⁴³Zie artikel 63, tweede lid, ook onder verwijzing naar artikel 61, eerste lid, onder d van het voorstel.

¹⁴⁴ Eventueel aangevuld met inzageverlening, door de van overeenkomstige toepassingsverklaring van artikel 66, derde lid. Terinzageverlening zou niet nodig zijn als met "mededeling" hier toch een vorm van verstrekking zou worden bedoeld.