Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

34 588 Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..)

Nr. 4

ADVIES AFDELING ADVISERING RAAD VAN STATE EN NADER RAPPORT[1]

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 21 september 2016 en het nader rapport d.d. 28 oktober 2016, aangeboden aan de Koning door de Minister van Binnenlandse Zaken en Koninkrijksrelaties, mede namens de Minister-President, Minister van Algemene Zaken en de Ministers van Defensie en van Veiligheid en Justitie. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

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

[1] De oorspronkelijke tekst van het voorstel van wet en van de memorie van toelichting zoals voorgelegd aan de Afdeling advisering van de Raad van State is ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

kst-34588-4
ISSN 0921 - 7371
's-Gravenhage 2016

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 bezien, daadwerkelijk effectieve bescherming biedt. Het wetsvoorstel schiet op dit punt tekort. De 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 onderzoeksopdrachtgerichte interceptie
   f. Vernietiging niet onderzochte gegevens
   g. Vernietiging niet relevante gegevens
   h. Vernietiging versleutelde gegevens
   i. Samenwerking buitenland
   j. Profilering 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

Blijkens de mededeling van de Directeur van Uw kabinet van 20 april 2016, no.2016000730, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 21 september 2016, nr. W04.16.0097/1, bied ik U hierbij aan, mede namens de Minister-President, Minister van Algemene Zaken, de Minister van Defensie en de Minister van Veiligheid en Justitie.

De Afdeling advisering van de Raad van State concludeert dat het wetsvoorstel een aanzienlijk aantal belangrijke waarborgen bevat waarmee voldaan wordt aan enkele essentiële vereisten van het EVRM. De Afdeling advisering 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 advisering op zichzelf legitiem: de noodzaak daarvan acht zij voldoende beargumenteerd.

De Afdeling advisering 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 advisering 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 acht de Afdeling advisering van wezenlijk belang voor de werking van de voorgestelde nieuwe Wet op de inlichtingen- en veiligheidsdiensten. De Afdeling advisering heeft bezwaar tegen de inhoud en opzet van het voorgestelde stelsel van toezicht en geeft in overweging dit voorstel van wet op dit punt niet aldus te zenden aan de Tweede Kamer der Staten-Generaal. Daarnaast is de Afdeling advisering niet overtuigd van de proportionaliteit van met name de grootschalige gegevensverzameling, in het bijzonder heeft de Afdeling advisering ernstige twijfels over de verenigbaarheid van de bewaartermijn van drie jaar met het EVRM. Zij ziet voorts geen reden om van strafrechtelijke handhaving af te zien. Tot slot gaat de Afdeling advisering in op enkele andere onderwerpen.

In het onderstaande zal op de verschillende onderdelen van het advies van de Afdeling advisering worden ingegaan.

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».[2] 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.[3] 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

---

[2] Aldus de toelichting, paragraaf 1.1.

[3] 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.

met de brandhaarden aan de randen van Europa.[4] Bepalend voor de omvang van die risico's zijn ook de hieraan gerelateerde technologische ontwikkelingen,[5] 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.[6]

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 proactief, met het 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.[7] 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.[8]

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.

---

[4] Zie in deze zin de toelichting, paragrafen 1.1 en 1.3.

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

[6] 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.»

[7] Toelichting, paragraaf 1.1.

[8] Dessens 2013, blz. 8.

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.[9]

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.[10] *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 EHRM*[11] *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.[12]

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 rechtmatigheids-

---

[9] Toelichting, paragraaf 1.2.

[10] 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.

[11] 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.

[12] Commissie Dessens, hoofdstuk 5.

oordelen 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 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,[13] 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.[14]

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.[15] 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.

1. Inleiding

a. Algemeen

b. Aanleiding voor het wetsvoorstel

c. Kabinetsstandpunt en wetsvoorstel

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.[16] 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

---

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

[14] Toelichting bij het consultatiewetsvoorstel, paragraaf 7.3.2.

[15] Artikelen 31 en 32 van het voorstel.

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

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 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.[17] Dit betekent dat eventuele beperkingen ten aanzien van een bepaald aspect veelal kunnen worden gecompenseerd door andere waarborgen.[18]

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 toezichtsstelsel (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.[19] 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.[20] 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 individu adequate

---

[17] 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.

[18] 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.

[19] Artikel 8 EVRM.

[20] 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.

bescherming te bieden tegen arbitraire inbreuken op zijn persoonlijke levenssfeer.[21]

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.[22] *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.*[23]

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 wetsvoorstel[24] *zien immers uitsluitend op het doel van de nationale veiligheid, los van strafrechtelijke connotaties.*[25] *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.*[26] *In de Telegraaf-zaak ten slotte oordeelde het Hof dat het op grond van artikel 6, tweede lid, onder a van de WIV 2002*[27] *afluisteren 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.*[28]

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.[29] *Zoals de toelichting uiteenzet*[30] *mogen slechts ter uitvoering van een deel van deze taken*[31] *bijzondere bevoegdheden die ingrijpende inbreuken op de persoonlijke levenssfeer maken, ingezet worden.*[32] *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.*

---

[21] EHRM 26 maart 1987, 9248/81, Leander t. Zweden, par. 51.

[22] 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; […].

[23] EHRM 1 juli 2008, 58243/00, Liberty t. Verenigd Koninkrijk, par. 64–69.

[24] De artikelen 8, tweede lid, en 10, tweede lid, van het voorstel.

[25] Vergelijk artikel 13 van het voorstel.

[26] EHRM 18 mei 2010, 26839/05, Kennedy t. Verenigd Koninkrijk, par. 159.

[27] 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».

[28] EHRM 22 november 2012, 39315/06, Telegraaf Media Nederland Landelijke Media B.V. e.a. t. Nederland, par. 90–93.

[29] De artikelen 8, tweede lid, en 10, tweede lid, van het voorstel.

[30] Toelichting, paragraaf 9.2.1.

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

[32] Artikel 28, eerste lid, van het voorstel, met een beperkte uitzondering in het tweede lid.

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.[33]

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.[34] *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 regering*[35] *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.*[36]

Wel moet worden bezien 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 beschikking staan tegen de inzet van bevoegdheden.[37] *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.*[38]

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

---

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

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

wordt op de grondrechten van burgers.[39] Daarbij moet ook worden bezien 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 diensten[40], 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.[41] Op de uitvoering van deze en andere bevoegdheden houdt de CTIVD toezicht.[42]

Verder bevat het voorstel waarborgen met betrekking tot de opslag, lengte van de bewaartermijnen en vernietiging van gegevens, die medebepalend zijn voor de verstrekkendheid 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.[43] Ten slotte bevat het voorstel een plicht tot notificatie[44] met betrekking tot het openen van brieven en andere zendingen[45], het «gericht tappen»[46] 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

---

[39] EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland.
[40] Bijvoorbeeld de bevoegdheid van toegang tot plaatsen als bedoeld in artikel 57.
[41] Ingevolge de artikelen 35 en 36 van het voorstel.
[42] Artikel 95, derde lid, van het voorstel.
[43] Zie punt 4 voor kritische kanttekeningen bij die specifieke regelingen
[44] Artikel 58 van het voorstel.
[45] Artikel 43 van het voorstel.
[46] Artikel 46 van het voorstel.

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.[47] *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.

2. Verenigbaarheid met het EVRM: toetsing op enkele hoofdlijnen

a. Inleiding: de aard van de toetsing

Op verzoek van de Tweede Kamer is aan de Afdeling advisering (hierna: de Afdeling) expliciet de vraag voorgelegd of het wetsvoorstel voldoet aan de eisen die voortvloeien uit het EVRM.

De Afdeling merkt daarbij terecht op dat de vraag of het wetsvoorstel voldoet aan die eisen niet eenvoudig en met zekerheid beantwoord kan worden. De uitspraken van het EHRM zien telkens op een concreet aan het Hof voorgelegde casus. Wel heeft het Hof inmiddels in enkele uitspraken enkele algemene uitgangspunten geformuleerd, zij het dat het EHRM – zoals de Afdeling terecht opmerkt – 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. Tegen deze achtergrond is het aangewezen op te merken dat het EHRM in diverse uitspraken heeft aangegeven dat het oordeel of een bepaalde stelsel EVRM-proof is, uiteindelijk alleen door het Hof kan worden vastgesteld.

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

c. Noodzakelijk in een democratische samenleving

De Afdeling is het met de regering 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 reeds toegelaten is) niet gehandhaafd kan worden, en dat mede gelet daarop de uitbreiding van de in het wetsvoorstel opgenomen bevoegdheden tot «bulk»-interceptie tot kabelgebonden communicatie in het licht van het EVRM gerechtvaardigd is. De Afdeling merkt aansluitend op dat wel moet worden bezien of wordt voldaan aan de vereiste van subsidiariteit en proportionaliteit. De Afdeling wijst vervolgens op de artikelen 18 en 26 van het wetsvoorstel waarin

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

deze eisen zijn geformuleerd als algemene uitgangspunten die door de diensten bij de uitoefening van bevoegdheden tot het verzamelen en verwerken van gegevens in acht moeten worden genomen. De door de Afdeling geuite veronderstelling dat deze algemene beginselen betrekking hebben op alle bevoegdheden van de diensten en steeds gelezen moeten worden in samenhang met het primaire doel van de diensten, het belang van de nationale veiligheid, is juist.

d. Tussenconclusie

e. Toezicht en Big Data

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.[48]

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.[49] *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).»[50]

---

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

[49] 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.

[50] Kamerstukken II 1999/2000, 25 877, nr. 8, blz. 108.

Het belang van een goed functionerende ministeriële verantwoordelijkheid en parlementaire controle betekent evenwel niet dat rechtmatigheidscontrole door een onafhankelijke toezichthouder niet nodig is.[51] De introductie in het wetsvoorstel van de TIB beoogt tegemoet te komen aan de kritiek die in de consultatiefase is geuit op het ontbreken van een voorafgaande onafhankelijke toetsing van de inzet van bijzondere bevoegdheden door de diensten.[52] In verschillende reacties werd gesteld dat zonder een dergelijke voorafgaande toets niet zou worden voldaan aan de vereisten die het EHRM stelt.[53]

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.[54]

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 wenselijk[55], maar sluit het andere vormen van toezicht, mits onafhankelijk en effectief, niet uit.[56] 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.[57] 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.[58]
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 in het geding zijn. Het afluisteren of tappen

---

[51] 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.

[52] 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.

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

[54] Toelichting, paragraaf 3.3.3.1.

[55] 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.

[56] 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.

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

[58] EHRM 18 mei 2010, 26839/05, Kennedy t. Verenigd Koninkrijk, par. 166–169 en 196.

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.[59] 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.[60]

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 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

---

[59] 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.»

[60] 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.»

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.[61] *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.*[62]

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 diensten[63] *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.*[64]

Het ligt gelet op het bovenstaande dan ook in de rede dat de toets door de TIB nagenoeg altijd positief zal uitvallen.[65] *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 operaties*[66]*, 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.*

---

[61] Venice Commission 2015b, par. 90.

[62] 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.

[63] 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.

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

[65] Zie de voorbeelden genoemd door Dessens 2013, blz. 97–98.

[66] Dat geldt bij uitstek voor de inzet van de (nieuwe) bevoegdheden tot onderzoeksopdrachtgerichte kabelgebonden interceptie (artikelen 47–49 van het voorstel).

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.[67] 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 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.

---

[67] Toelichting, paragraaf 9.2.1 Toetskader artikel 8 EVRM, *Voorzienbaarheid: de toestemmingssystematiek.*

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.[68] 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.[69]

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

Vervolgens moet worden bezien 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.[70]

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

---

[68] 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.

[69] 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.

[70] 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.

oordeel van de CTIVD,[71] 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.[72] 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 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)[73]) in het licht van het EVRM voldoet.[74] 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.[75]

e. Klachtrecht

De behandeling van klachten is in de huidige Wiv 2002 belegd bij de Nationale ombudsman.[76] 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.[77]

---

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

[72] Daarbij is het overigens onvermijdelijk dat de CTIVD slechts steeksproefsgewijs die praktijk zal kunnen onderzoeken.

[73] Waarover hierna meer in punt e.

[74] 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.

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

[76] 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.

[77] Toelichting paragraaf 9.5.

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 wordt vermeden.»[78] 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.[79] 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.[80] 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 correctie[81] met bijbehorende bestuursrechtelijke rechtsbescherming. Voor zover deze bepalingen onvoldoende inzage- en correctierecht zouden bieden ligt het veeleer voor de hand deze aan te passen.[82] Daar komt bij dat het laatste oordeel over de rechtmatigheid van de procedure en de inzet van de bevoegdheden aan de rechter is.[83] 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

---

[78] Advies van 17 september 1997, Kamerstukken II 1997/98, 25 877, A.

[79] 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.

[80] Toelichting, paragraaf 9.5.

[81] De artikelen 47–56 van de Wiv 2002, respectievelijk de artikelen 74–83 van het voorstel.

[82] 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.

[83] 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.

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.

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.[84] 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 bezien 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.

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

3. Effectief toezicht

a. Straatsburgse rechtspraak: hoofdlijnen

De Afdeling geeft een schets op hoofdlijnen van de Straatsburgse rechtspraak, waarbij zij, waar het gaat om het belang van adequaat *toezicht*, zich uitsluitend (lijkt te) richt(en) op de eisen die ter zake uit artikel 13 EVRM voortvloeien. Artikel 13 EVRM eist dat een ieder wiens rechten en vrijheden die in het EVRM zijn vermeld, zijn geschonden, recht heeft op een daadwerkelijk rechtsmiddel voor een nationale instantie, ook indien deze schending is begaan door personen in de uitoefening van hun ambtelijke functie. Opvallend is dat in de beschouwing van de Afdeling niet wordt ingegaan op een van de eisen die in het kader van artikel 8 EVRM is ontwikkeld, en die vaak in samenhang met artikel 13 EVRM dient te worden beschouwd. Zo wordt aan de (veelal heimelijke) bevoegdheidsuitoefening van inlichtingen- en veiligheidsdiensten de eis gesteld van de aanwezigheid van «*effective guarantees against abuse*» (effectieve waarborgen tegen misbruik); zie in dit verband onder meer *Klass e.a. tegen Duitsland* (EHRM 6 september 1978, par. 50). Dergelijke waarborgen dienen er onder meer te zijn in de sfeer van de autorisatie van de toepassing van bevoegdheden; dat kan zijn door de autorisatie in handen te leggen van een onafhankelijke instantie. Ook een toets op het autorisatieproces, zoals in het wetsvoorstel in handen is gelegd van de TIB, en rechtmatigheidstoezicht door bijvoorbeeld de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD), dient in die context te worden geplaatst.

b. Artikel 13 EVRM: «effectief» toezicht

De Afdeling geeft een uiteenzetting over wat naar haar mening onder «effectief» toezicht dient te worden verstaan. De toezichthoudende instantie(s) zou(den) niet alleen juridische kennis en vaardigheid moeten hebben, maar ook inzicht en overzicht van het feitelijk handelen van de diensten. Dat vergt een structureel inzicht in de wijze van werken van de diensten, hetgeen slechts verworven zou kunnen worden in een langdurige en continue toezichtsrelatie met de diensten. Voorts dient de toezichthouder – wil het toezicht in die relatie werkelijk effectief kunnen zijn – volledige inzage te hebben in en onbeperkte toegang te hebben tot de informatiesystemen van de diensten. Een effectieve toezichthouder, aldus de Afdeling, dient derhalve over aanzienlijke informatie- en onderzoeksbevoegdheden te beschikken. Ook vereist effectief toezicht dat alle fasen in de werkzaamheden van de diensten moeten kunnen worden gecontroleerd. Fases van gegevensverwerking die in de praktijk nauw met elkaar zijn verweven. Dit leidt bij de Afdeling tot de conclusie dat dit vraagt om een sterke toezichthouder die zicht heeft op het grote geheel en de samenhang tussen de verschillende onderdelen. Daaraan voegt zij voorts toe dat voor de beoordeling van de rechtmatigheid van de toestemming het derhalve noodzakelijk is 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.

Bij dit betoog, waarbij grotendeels wordt geput uit een rapportage van de Venice Commission uit 2015 (*Report on the democratic oversight of security services*), moet naar het oordeel van de regering worden betrokken het gegeven dat het EHRM – zoals door de Afdeling ook eerder is gesteld – naar het stelsel als geheel kijkt, waar het gaat om de vraag of er sprake is van effectief toezicht. De jurisprudentie van het EHRM laat

zien, dat verschillende soorten invullingen van de eis van effectief toezicht bestaan en adequaat zijn geacht. Daarbij is ruimte voor verschillende instanties, in verschillende fasen van het onderzoek van de diensten en met op die fasen toegesneden bevoegdheden.

c. Effectiviteit van de toetsing door de TIB

De Afdeling is niet overtuigd van de effectiviteit van de toetsing door de TIB.
De TIB is inderdaad slechts gepositioneerd aan de voorkant van het proces, te weten in het autorisatieproces voor de uitoefening van de meest vergaande bijzondere bevoegdheden van de dienst (waarvoor in het wetsvoorstel de toestemming van de Minister is vereist, zonder de mogelijkheid van mandaat). Daarnaast blijft de CTIVD toezicht houden op alle fases van de inzet van bijzondere bevoegdheden. De rol van de TIB is een andere dan die van de CTIVD. De TIB toetst of een door de Minister genomen besluit rechtmatig is; dat betekent een toets aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Anders dan de Afdeling schetst, is dit geen zeer marginale en abstracte rechtmatigheidsbeoordeling. Het gaat immers om meer dan alleen bezien of de voorgeschreven procedures zijn gevolgd en de Minister in redelijkheid tot het besluit had kunnen komen. De TIB zal immers hetzelfde feitencomplex als de Minister krijgen voorgelegd en de in dat kader beoogde bevoegdheidsuitoefening in zijn volle omvang aan een rechtmatigheidstoets kunnen onderwerpen. De toets door de TIB is voorts een eenmalige toets op een besluit en derhalve van een heel andere orde dan het toezicht dat door de CTIVD wordt uitgeoefend, waarbij de uitvoering door de diensten van hun taak en bevoegdheden doorlopend kan en moet kunnen worden gemonitored. Voor dat laatste is inderdaad vereist dat er bijvoorbeeld rechtstreeks toegang is tot alle gegevens bij de diensten en dat er zicht is op de samenhang van de uitoefening van verschillende bevoegdheid en de gevolgen voor de uitvoeringspraktijk; voor de toets door de TIB is dat niet (in die mate) vereist. De TIB kan volstaan met de informatie die ook de Minister is voorgelegd bij het nemen van het besluit, zij het dat de TIB wel het recht heeft om alle informatie die zij nodig acht voor haar taak bij de Minister op te vragen.

De Afdeling merkt voorts op dat met de introductie van de rechtmatigheidstoets door de TIB afbreuk kan worden gedaan aan de ministeriële verantwoordelijkheid voor de diensten. Ter zake wordt het volgende opgemerkt. Terecht 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. Die beslissing is niet onderworpen aan de toets door de TIB noch aan het rechtmatigheidstoezicht door de CTIVD. De Minister draagt voor die beslissing de volle ministeriële verantwoordelijkheid. Het vervolgens uitvoeren van het onderzoek brengt met zich mee dat – afhankelijk van de onderzoeksvraag, de onderzoeksmogelijkheden e.d. – overgegaan dient te worden tot de inzet van bijzondere bevoegdheden. Voor die inzet zal toestemming van de Minister (of een andere bij of krachtens de wet aangewezen instantie) moeten worden verkregen, waarbij niet alleen zal dienen te worden aangetoond dat die inzet noodzakelijk is, maar ook dat deze proportioneel (evenredigheid doel en middel) en subsidiair (van de beschikbare middelen het middel dat de minste inbreuk maakt). Bij de toets aan laatstgenoemde criteria is het niet geheel uit te sluiten dat andere componenten die in de beleidsmatige afweging een rol spelen ook daarin doorwerken. Afbreukrisico bij ontdekking van de inzet van een bijzondere bevoegdheid, de hoedanigheid van het target, de urgentie van het onderzoek, de (praktische) mogelijkheden tot inzet van de bevoegdheid en dergelijke zijn uiteraard aspecten die een rol zullen spelen

bij de keuze van welke bevoegdheid moet c.q. kan worden ingezet – en met welke intensiteit en duur – gelet op het relevante complex aan feiten. Maar, uiteindelijk wordt wel gekozen voor de inzet van een bepaalde bevoegdheid die de rechtmatigheidstoets dient te doorstaan. Dat moet in het verzoek om toestemming worden verantwoord en de Minister (of een andere bij of krachtens de wet aangewezen instantie) zal daarop bij diens besluitvorming acht moeten slaan; het gaat immers om toepassing van wettelijk vastgelegde eisen. De Minister is volledig verantwoordelijk voor het uiteindelijk door hem genomen besluit.
Dat een bindende toets door de TIB leidt tot een inperking van de ministeriële bevoegdheid en daarmee ook een inperking van de ministeriële verantwoordelijkheid en de daarmee samenhangende mogelijkheid tot parlementaire controle is voor discussie vatbaar. Voor zover de introductie van de TIB als een dergelijke beperking zou kunnen worden opgevat, geldt, dat het uiteindelijk de wetgever is die bewust daarvoor kiest. De wetgever aanvaardt en beoogt daarmee, dat indien de Minister niet in staat is om de rechtmatigheid van een besluit (noodzaak, proportionaliteit en subsidiariteit) te onderbouwen, de uitoefening van een bijzondere bevoegdheid waarmee inbreuk op iemands grondrechten kan worden gemaakt, achterwege dient te blijven. De Minister kan immers altijd een nieuw besluit nemen, waarbij gepoogd kan worden de door de TIB geconstateerde gebreken op het vlak van rechtmatigheid (onvoldoende noodzaak aangetoond, disproportioneel of een te zwaar middel als er een lichter alternatief voorhanden is) weg te nemen. Of de Minister daarvoor kiest is ook aan de Minister en ook daarvoor is hij verantwoordelijk. Voorts is de Minister volledig verantwoordelijk voor de uiteindelijke uitvoering van de bijzondere bevoegdheid. De parlementaire controle blijft intact.

De Afdeling komt uiteindelijk tot haar oordeel dat de keuze tot invoering van de TIB, ondanks het feit dat de invoering daarvan in formele zin voldoet aan de jurisprudentie van het EHRM, ernstig moet worden ontraden, omdat niet wordt voldaan aan de eis van daadwerkelijke effectiviteit (materiële gronden). Dit oordeel wordt om redenen zoals hiervoor uiteengezet, niet gedeeld. De TIB zal dan ook in het wetsvoorstel worden gehandhaafd, waarbij de door de Afdeling in onderdeel 7 van haar advies gedane voorstellen voor de vormgeving van de TIB zullen worden verwerkt.

Tot slot vraagt de Afdeling zich af of en hoe de werkzaamheden van de TIB en de CTIVD op elkaar moeten worden afgestemd. De Afdeling acht niet uitgesloten dat de TIB en de CTIVD op verschillende momenten tot verschillende oordelen komen over de rechtmatigheid van een interceptie of een gegevensverwerking. Het voorgestelde systeem leidt naar de overtuiging van de Afdeling tot een te gefragmenteerd stelsel dat afbreuk doet aan de vereiste effectiviteit van het toezicht. Dit oordeel van de Afdeling wordt niet gedeeld. De TIB en de CTIVD hebben ieder een verschillende rol in een verschillende fase van de taakuitvoering van de diensten. De CTIVD houdt toezicht tijdens en achteraf op de rechtmatige uitvoering van de wet en behandelt klachten hierover, terwijl de TIB een bindende toets uitvoert voorafgaand aan de inzet van bepaalde bijzondere bevoegdheden. Nu de toets op de rechtmatigheid van het door de Minister genomen besluit voorafgaand aan de inzet van een bijzondere bevoegdheid exclusief bij de TIB is belegd, brengt dat met zich mee dat de CTIVD de rechtmatigheid van dat besluit in beginsel dient te respecteren; slechts indien de CTIVD in het kader van haar toezicht op de uitvoering van een dergelijk besluit constateert dat het door de Minister genomen besluit en het voor toetsing aan de TIB voorgelegde besluit is gebaseerd op onvolledige of onjuiste informatie, kan zij dit als bevinding aan de

Minister rapporteren. De Minister zal dan dienen te bezien of er aanleiding is een nieuw besluit te nemen en dat (opnieuw) aan de TIB voor te leggen.

De memorie van toelichting is waar nodig naar aanleiding van het voorgaande aangevuld.

d. Effectiviteit van het toezicht door de CTIVD

De Afdeling komt naar aanleiding van haar overwegingen in onderdeel 3c van haar advies tot de conclusie dat het voor de hand ligt om de CTIVD, de huidige toezichthouder, als de gespecialiseerde instantie aan te wijzen die toezicht houdt over het geheel. In de reactie op hetgeen de Afdeling in onderdeel 3c naar voren heeft gebracht, is gemotiveerd aangegeven dat de TIB in het stelsel zal worden gehandhaafd. Ook is daarbij ingegaan op de rol van de TIB en de CTIVD in het toezichtstelsel als geheel.

e. Klachtrecht

De Afdeling – onder verwijzing naar het advies van de Raad van State ten aanzien van het oorspronkelijke ontwerp voor de Wiv 2002 uit 1996 – acht de bezwaren die indertijd zijn geuit tegen het voorstel om de CTIVD als externe klachtbehandelaar aan te wijzen, nog steeds geldig. Toezicht en onafhankelijke klachtbehandeling dienen strikt gescheiden te zijn, opdat zelfs de schijn van partijdigheid wordt vermeden.

Om (de schijn van) partijdigheid te vermijden is in het wetsvoorstel voorzien in een scheiding tussen de afdeling toezicht en de afdeling klachtbehandeling die bij de CTIVD worden ingesteld. Dit brengt met zich mee dat leden van de afdeling toezicht niet tegelijkertijd lid kunnen zijn van de afdeling klachtbehandeling en omgekeerd.

Waar het gaat om het voorstel om te komen tot de introductie van een bindende klachtbevoegdheid wijst de Afdeling naar hetgeen in paragraaf 9.5 van de memorie van toelichting is gesteld, waarbij met name ingegaan wordt op het arrest van het EHRM in de zaak *Segerstedt-Wiberg tegen Zweden*. De Afdeling relativeert het belang daarvan.
Bij de voorbereiding van het wetsvoorstel en in het bijzonder bij het vormgeven van het stelsel van toezicht is nadrukkelijk acht geslagen op het Britse systeem, waarbij immers – vergelijkbaar met Nederland – de ministers de besluiten tot de inzet van bevoegdheden nemen en daarop wordt toegezien door de eerder genoemde *commissioner*. Daarnaast wordt voorzien in bindend klachtrecht. In het arrest *Kennedy* is door het EHRM het Britse systeem als geheel (dus inclusief het bindend klachtrecht) in overeenstemming geacht met het EVRM. De in het wetsvoorstel opgenomen klachtvoorziening is mede daardoor geïnspireerd.

De Afdeling acht, gelet op het feit dat bij de beoordeling of sprake is van een daadwerkelijk rechtsmiddel in de zin van artikel 13 EVRM er naar het geheel van beschikbare voorzieningen dient te worden gekeken, de conclusie over het vereiste van bindende oordelen door een klachtinstantie te absoluut en te generiek. Voorts wijst de Afdeling erop dat het laatste oordeel over de rechtmatigheid van de procedure en de inzet van de bevoegdheden aan de rechter is.
Bij de voorbereiding van het wetsvoorstel is de vraag of overgegaan moet worden tot de invoering van een bindend klachtrecht bevestigend beantwoord. Daarbij is de inschatting gemaakt dat het bestaande stelsel – ook als geheel bezien – in het licht van artikel 13 EVRM te kwetsbaar is. Weliswaar bestaat voor de burger de mogelijkheid om naar aanleiding van een onbevredigende afhandeling van een inzageverzoek de rechtsmiddelen uit de Algemene wet bestuursrecht te benutten of bij een

(vermeend) onrechtmatige daad van de diensten de civiele rechter te adiëren, maar zeker dit laatste – zo leert de praktijk – is problematisch. Voor de burger is het lastig aan te tonen dat er daadwerkelijk sprake is van een onrechtmatige daad en voor de Staat is het lastig om dit effectief tegen te spreken, nu daarmee mogelijk inzicht (moet) worden gegeven in bronnen, modus operandi en actueel kennisniveau. Mede in dat licht bezien is het wenselijk geacht om het Nederlandse stelsel aan te vullen met een laagdrempelige voorziening, waarbij door de afdeling klachtbehandeling een effectief en bindend oordeel kan worden gegeven. Anders dan de rechter heeft de afdeling klachtbehandeling – evenals de afdeling toezicht – recht op toegang tot alle gegevens bij de diensten en kan dus op basis van alle feiten een oordeel uitspreken. Vanzelfsprekend blijft een gang naar de rechter openstaan.

f. Conclusie

De Afdeling komt tot het oordeel dat het voorgestane stelsel van toezicht als geheel niet toereikend is. Dit oordeel is in reactie op de verschillende oordelen gemotiveerd weerlegd. Er wordt dan ook afgezien van aanpassing van het wetsvoorstel, zoals door de Afdeling is voorgesteld, te weten door schrapping van de TIB en door de klachtregeling zoals in de Wiv 2002 is neergelegd te handhaven. Daar komt ten slotte nog bij dat het EVRM (en de jurisprudentie van het EHRM) een minimum-norm formuleren; het staat aan de verdragsstaten altijd vrij om in meer waarborgen te voorzien. Zoals de Afdeling ook eerder in haar advies heeft aangegeven is het Nederlandse stelsel nimmer ten gronde door het EHRM beoordeeld. Met het thans in het wetsvoorstel neergelegde stelsel, zowel waar het gaat om de introductie van de TIB (die conform het advies van de Afdeling is versterkt)[85] als de invoering van bindend klachtrecht, wordt een dergelijke beoordeling met vertrouwen tegemoet gezien.

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

[85] Zie advies, p. 36.

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.[86]

Het gebruik van Big Data heeft, zo wordt ook door de WRR onderstreept, een grote potentie.[87] 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 gerichter 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.[88] 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 categori-

---

[86] WRR, *Big Data in een vrije en veilige samenleving*, Amsterdam University Press, Den Haag/Amsterdam 2016 (hierna: WRR 2016), blz. 21.
[87] WRR 2016, blz. 76 e.v.
[88] WRR 2016, blz. 88.

sering 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.[89] 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 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.[90]

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 telecomaanbieders 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.[91] 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.[92] Deze strenge koers van het Hof van Justitie met het oog op de bescherming van persoonsgegevens is in latere arresten voortgezet.[93] Hoewel het EU-recht en de rechtspraak van het Hof niet van toepassing zijn op de diensten,[94] is aannemelijk dat de daarin geformuleerde uitgangspunten

---

[89] WRR 2016, blz. 82.

[90] WRR 2016, blz. 137.

[91] 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 Kärtner Landesregierung).

[92] Digital Rights Ireland, punten 57–59.

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

[94] Zie de artikelen 72 en 276 van het VWEU.

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.[95] 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 ongedifferentieerde en allesomvattende intercepties mag plegen en persoonsgegevens mag opslaan en raadplegen.[96]

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.[97]

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.

---

[95] «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.

[96] 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.

[97] Met betrekking tot de onderzoeksopdrachtgerichte interceptie vooral paragraaf 3.3.4.4.7.4 en bijlage 4 van de toelichting.

c. Transparantie werkwijze

De WRR heeft in haar eerder genoemde rapport aanbevolen dat er meer transparantie moet komen over de dataverwerkingsprocessen van de overheid.[98] Voor burgers is ook door de moderne techniek de gegevensverwerking door de 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 aanzienlijker 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.[99] In dat verband memoreert de WRR de discussie over de geheimhouding van tapstatistieken.[100] Tegen deze achtergrond adviseert de Afdeling om uitgebreider[101] 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 voorbewerking 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 van

---

[98] WRR 2016, blz. 144.
[99] WRR 2016, blz. 145.
[100] Zie ABRvS 13 januari 2016, nr. 201409649/1A3.
[101] De toelichting is thans te summier. Zie paragraaf 1.2.2.

onderzoek (artikel 49). In deze fase kan ook geautomatiseerde data-analyse worden toegepast (artikel 59).[102]

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.[103] *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 volgordelijkheid, 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 geformuleerd*[104] *en daardoor minder waarborgen zal bieden dan uit het wetsvoorstel zou kunnen worden afgeleid. In de toelichting wordt dit onderkend,*[105] *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 onderzoeksopdrachtgerichte interceptie

In de toelichting wordt de kritiek op het conceptwetsvoorstel dat de bevoegdheid tot onderzoeksopdrachtgerichte 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 onderzoeksopdrachtgerichte interceptie van grote hoeveelheden data.[106] *Die ruime schaal is mede nodig omdat het onderzoek ook gericht kan zijn op nog (nagenoeg) ongekende dreigingen. Daarbij zal de interceptie blijkens de toelichting plaatsvinden op een bepaald onderzoeksgebied of thema (bijvoorbeeld 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.*[107]

---

[102] Toelichting, paragraaf 3.3.4.4.7.4.

[103] Reactie CTIVD, blz. 26 e.v.

[104] Dat 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.

[105] Toelichting, paragraaf 3.3.4.4.7.4

[106] Toelichting, paragraaf 12.2.

[107] Toelichting, paragraaf 3.3.4.4.7.4

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.[108] Daarbij sluit de PIA aan bij Jacobs, die een twee fasen-model volgens het principe «select while you collect» heeft voorgesteld.[109] 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.[110]

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 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.[111] 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.

---

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

[109] Bart Jacobs, «Select while you collect. Een bespreking van interceptie door inlichtingen- en veiligheidsdiensten», *NJB* 2016, blz. 256–261.

[110] EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 255.

[111] Toelichting, paragraaf 12.2.

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.[112]

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 privéleven. 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 privéleven 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.[113] 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 wijze waarop het dataverkeer kan worden verzameld voor de begrenzing van de gegevens die zij daadwerkelijk binnenkrijgen.[114] De bewaartermijn moet ten slotte worden bezien 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.[115]

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.[116] Het recht op bescherming van het privéleven 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

---

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

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

114 Bijvoorbeeld in het geval een onderzoeksopdracht 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.

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

116 Toelichting, paragraaf 3.3.4.4.7.4.

jaar in dit geval noodzakelijk en proportioneel is in een democratische samenleving als bedoeld in artikel 8, tweede lid, EVRM.[117] 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.[118] Weliswaar bevat het wetsvoorstel daarover regels[119] 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 onderzoeksopdrachtgerichte interceptie van kabelgebonden verkeer zijn verkregen. Het artikel lijkt, ook gelet op de toelichting, te impliceren dat gegevens die onderzocht zijn en binnen die onderzoeksopdracht 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 onderzoeksopdrachtgerichte interceptie zijn verzameld. Dit eerste lid bepaalt onder meer dat gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het 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 onderzoeksopdrachtgerichte 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[120] – vernietiging van gegevens een belangrijke waarborg is tegen een te grote inbreuk op het recht op bescherming van het privéleven, 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.

---

[117] 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.

[118] EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 255.

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

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

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 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, eerde 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.[121] 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

[121] «Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten», Universiteit Leiden, blz. 28.

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.[122]

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 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 gedoeld 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».[123]

Het in artikel 59, derde lid, neergelegde verbod sluit aan bij bestaande[124] *en toekomstige*[125] *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.*[126]

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 interceptie[127]*, niet moet worden verbreed tot alle vormen van geautomatiseerde data-analyse. De algemene, in artikel 18, derde lid, neergelegde*

---

[122] Rapport van de CTIVD nr. 49 over de uitwisseling van ongeëvalueerde gegevens door de AIVD en de MIVD.
[123] Toelichting, paragraaf 3.5.
[124] Artikel 15 Richtlijn 95/46/EG.
[125] Artikel 22 Verordening (EU) 2016/679 (Algemene verordening gegevensbescherming). Deze verordening zal in 2018 Richtlijn 95/46/EG vervangen.
[126] WRR 2016, blz. 132–133.
[127] Zie artikel 49, eerste lid, onder b, van het voorstel.

zorgplicht[128] 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.

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).[129] 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).[130]

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.[131] 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.[132]

---

[128] 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.

[129] PIA, blz. 158. Zie voor een nadere onderbouwing blz. 148 e.v.

[130] Toelichting, paragrafen 12.3.2.3 en 3.2.6

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

[132] Artikel 25 Verordening (EU) 2016/679.

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 het globale kader van uitgangspunten[133] 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.

4. Gegevensverwerking: Big Data

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

b. Een samenhangende visie

De Afdeling onderkent in haar advies het belang en de potentie van Big data voor de bevoegdheden van de inlichtingen- en veiligheidsdiensten, maar wijst tegelijkertijd op de risico's die met het gebruik ervan gepaard kunnen gaan. Zij baseert zich daarbij grotendeels op het rapport van de WRR getiteld «Big data in een vrije en veilige samenleving».[134] Om het politieke en maatschappelijke vertrouwen van de diensten blijvend te kunnen behouden is volgens de Afdeling 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 technologische ontwikkelingen. Grootschalige verwerking van gegevens door de diensten kan ertoe leiden dat burgers het gevoel krijgen dat hun persoonlijke levenssfeer wordt beperkt. Dat kan ertoe leiden dat zij hun gedrag aanpassen. De Afdeling vraagt aandacht voor het feit dat data-analyses fouten kunnen bevatten en kunnen leiden tot verkeerde conclusies hetgeen het risico van mogelijk onevenredige gevolgen zoals discriminatie kan versterken. Ook wijst de Afdeling op het feit dat de technologische ontwikkelingen gevolgen hebben voor de toepassing van basisprincipes als doelbinding en noodzakelijkheid van de verwerking van gegevens. Tot slot wijst de Afdeling in dit onderdeel van haar advies op recente EHRM-rechtspraak, die zich volgens de Afdeling kritisch heeft getoond in gevallen waarin de overheid ongedifferentieerde en allesomvattende datasets met persoonsgegevens mag opslaan en raadplegen.[135] De Afdeling verzoekt de regering in haar advies om in een beschouwing weer te geven op welke wijze wordt omgegaan met de invloeden van de technologische ontwikkelingen op de bevoegdheden van de diensten.

De regering verwelkomt de inleidende observaties van de Afdeling ter zake van de ontwikkelingen in het huidige dynamische technologische tijdgewricht.[136] Deze observaties lopen grotendeels samen met de

---

[133] Zie met name paragraaf 3.1 Algemene bepalingen ter zake van de verwerking van persoonsgegevens (artikelen 17–24 van het voorstel).
[134] WRR-rapport no. 95 (april 2016).
[135] *Szabo en Vissy tegen Hongarije*, EHRM 12 januari 2016, no. 37138/14, par. 66–69 en 89.
[136] Zie advies, p. 22.

waarnemingen in het eerdergenoemde WRR-rapport. Voor wat betreft de aanbevelingen uit het WRR-rapport wordt nader ingegaan op de adviezen die zijn gericht aan de inlichtingen- en veiligheidsdiensten in paragraaf 5.3 van de memorie van toelichting bij dit wetsvoorstel, dat ziet op geautomatiseerde (Big-)data analyse door de diensten. Hier wenst de regering te benadrukken dat zij zich duurzaam wil inzetten voor het vertrouwen dat de samenleving in big data-verwerking door de diensten moet kunnen stellen. De overheid heeft steeds de plicht om haar burgers te beschermen en hun veiligheid te vergroten opdat zij in vrijheid kunnen leven. Zij moet met het oog op het garanderen van die vrijheid zorg dragen voor de maatschappelijke en individuele veiligheid onder meer door informatie in te winnen, waakzaam te zijn en bronnen van onveiligheid te bestrijden. Daarbij kan Big data van grote waarde zijn. De regering is het met de Afdeling eens dat de inzet van Big data door de inlichtingen- en veiligheidsdiensten al tot positieve resultaten heeft geleid.

Big data-verwerking in het veiligheidsdomein brengt gelet op de aard van de verwerking echter ook de door de Afdeling gesignaleerde risico's met zich mee. In het eerste en enkele andere hoofdstukken van de memorie van toelichting wordt meer algemeen ingegaan op de betekenis van de technologische ontwikkelingen voor de bevoegdheden van de diensten.[137] In het wetsvoorstel worden gegevensverwerkingen, juist gelet op deze technologische ontwikkelingen in al hun onderdelen vanuit grondrechtelijke en mensenrechtelijke maatstaven herijkt en van passende waarborgen voorzien. Gelet op de toegenomen betekenis van verwerkingen met een Big data-karakter en naar aanleiding van de PIA Wiv en het advies van de Afdeling achtte de regering het dan ook noodzakelijk om geautomatiseerde data-analyse als werkmethode van de diensten van een expliciete wettelijke grondslag te voorzien. Het voorgestelde artikel 60 strekt hiertoe. Voor zover door de diensten geheel nieuwe technieken – zoals machinaal leren – voor geautomatiseerde data-analyse kunnen worden ingezet, zal dat gepaard dienen te gaan met een daaraan voorafgaande verkenning van de mogelijkheden die een dergelijke nieuwe techniek biedt, de voor- en nadelen inclusief de mogelijke privacyrisico's.

De resultaten van de analyses die worden verricht door de inlichtingen- en veiligheidsdiensten kunnen, zoals de Afdeling terecht stelt, een grote impact hebben voor de burgers die in een dergelijk onderzoek worden betrokken. Uitkomsten van geautomatiseerde processen van gegevensverwerking vereisen gelet op het feit dat zij correlaties weergeven, en geen causale verbanden, altijd menselijke validatie of nadere weging. Het resultaat van de analyse is bovendien afhankelijk van de (kwaliteit van de) gehanteerde algoritmen en data. De Afdeling wijst in haar advies terecht op de mogelijkheid dat geautomatiseerde data-analyse fouten kan bevatten die kunnen leiden tot verkeerde conclusies. Een menselijke afweging van het resultaat in het licht van andere onderzoeksgegevens (en een collegiale toets waar nodig) is juist bij het werk van inlichtingen- en veiligheidsdiensten van het grootste belang. Het benutten van data-analyses betreft een activiteit waarbij voortdurend sprake is van weging, inschatting en interpretatie van onderzoeksresultaten in combinatie met elkaar en in het licht van de specifieke onderzoeksvraag. Bovendien heeft de onafhankelijke toezichthouder toegang tot gegevensverwerkingsprocessen gedurende de gehele verwerkingscyclus, en kan deze beoordelen of op juiste wijze invulling wordt gegeven aan het verbod, zoals vastgelegd in artikel 60, derde lid, van het wetsvoorstel.

---

[137] Zie met name paragrafen 1.3 (waarom modernisering van bevoegdheden), 1.4 (nadere achtergronden bij de ontwikkelingen die dit wetsvoorstel noodzakelijk maken), 3.3.3 (De Toetsingscommissie inzet bevoegdheden), par. 3.3.4.4.7.4 (onderzoeksopdrachtgerichte interceptie van communicatie) en 5.3 (geautomatiseerde (big-)data analyse door de diensten).

c. Transparante werkwijze

De Afdeling adviseert – ook in lijn met het WRR-rapport – om transparantie in de dataverwerkingsprocessen (waartoe Big data ook wordt gerekend) van de overheid te vergroten teneinde het vertrouwen van de samenleving in de zorgvuldigheid en proportionaliteit van Big data gegevensverwerking te behouden. Hoewel het noodzakelijk heimelijke karakter van de gegevensverwerking – inclusief Big data- in het kader van de taken van de Wiv ertoe leidt dat de regering het uitgangspunt hanteert dat er geen volledige transparantie kan bestaan jegens eenieder voor wat betreft inzage in de gehanteerde werkmethoden van de diensten, geeft zij graag nadere invulling aan het advies met betrekking tot transparantie omdat zij het belang van het behoud van het vertrouwen van de samenleving in de Big data-verwerking door de diensten ten volle onderschrijft. Teneinde de transparantie over de Big data-verwerkingen te vergroten zet de regering in op het robuuster maken van twee instrumenten, te weten de jaarplannen van de AIVD en de MIVD en verdere capacitaire versteviging van het onafhankelijke toezicht. De jaarplannen van de diensten zullen met het oog op transparantie met betrekking tot Big data-verwerkingen worden aangevuld met een paragraaf over het gebruik van Big data, waarbij specifiek aandacht wordt besteed aan de doelen en frequentie van het gebruik van Big data en de mate waarin deze verwerkingen hebben bijgedragen aan het boeken van resultaten en het ontdekken van trends. Daarnaast zal worden beschreven of mitigerende maatregelen getroffen moesten worden om afwijkingen in de gegevensbronnen en analyses te corrigeren, teneinde een zinvolle analyse en daaruit voortvloeiende besluitvorming tot stand te kunnen brengen. De jaarplannen zijn vanwege hun inhoud staatsgeheim en worden integraal gedeeld met de Commissie voor de Inlichtingen- en Veiligheidsdiensten. De hoofdlijnen van de jaarplannen zullen onder de aandacht van burgers worden gebracht op de websites van de diensten.[138]
Daarnaast zal de TIB die voorafgaand de uitvoering van de bijzondere bevoegdheden toetst op rechtmatigheid worden versterkt zoals uitgelegd onder punt 7. Daarbij ontstaat ruimte om experts op het terrein van Big data-analyses te betrekken. Hetzelfde geldt voor de uitbreiding van de capaciteit van de CTIVD.

d. Driefasenaanpak en toestemming

In de memorie van toelichting is nader aangegeven dat de drie fasen, waaruit het nieuwe normatieve kader voor onderzoeksopdrachtgerichte interceptie bestaat, nauw met elkaar zijn verweven. Deze drie fasen zijn echter wel van elkaar te onderscheiden, maar in de praktische uitvoering – onder meer vanwege het feit dat de resultaten van de ene fase betrokken zullen worden bij de wijze waarop de bevoegdheden in de andere fasen kunnen worden uitgevoerd – zullen zij echter bij voortduring elkaar beïnvloeden. Voorts is naar aanleiding van de opmerkingen van de Afdeling in de memorie van toelichting nader ingegaan op de combinatie-last (combi-last).

e. Uitwerking onderzoeksopdrachtgerichte interceptie

De Afdeling wijst op het feit dat de wijze waarop aan artikel 27, eerste lid, in relatie tot de onderzoeksopdrachtgerichte interceptie uitvoering wordt gegeven, van cruciaal belang is. De toelichting maakt naar het oordeel van de Afdeling onvoldoende duidelijk hoe in de eerste fase (de interceptie), de bulk aan gegevens wordt gereduceerd tot die gegevens die voor verder onderzoek relevant kunnen zijn, hoe groot de hoeveelheid gegevens is die

[138] Zie bijv. https://www.aivd.nl/onderwerpen/het-werk-van-de-aivd/inhoud/de-aivd-en-privacy.

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.
Mede naar aanleiding van de opmerking van de Afdeling in onderdeel 4g in haar advies is waar het gaat om onderzoeksopdrachtgerichte interceptie in artikel 48, vijfde lid, van het wetsvoorstel thans voorzien in een zelfstandige regeling van het onderzoek op relevantie en de vernietiging van gegevens. Artikel 27, eerste lid, speelt hierbij dus geen rol meer. Naar aanleiding van de opmerking van de Afdeling is paragraaf 3.3.4.4.7.4 van de memorie van toelichting aangevuld met een beschouwing over de wijze waarop datareductie binnen het proces van onderzoeksopdrachtgerichte interceptie plaatsvindt. Waar het gaat om onderzoeksopdrachtgerichte interceptie op de kabel bestaat de verwachting (naar huidig inzicht) dat 95 tot 98% van de geïntercepteerde data reeds in de eerste fase zal worden vernietigd. De memorie van toelichting is ter zake aangevuld.

Voorts wijst de Afdeling erop dat aan het door Jacobs voorgestelde uitgangspunt van «select while you collect» «op hoofdlijnen» recht wordt gedaan, maar anderzijds ook (deels) wordt afgewezen. Niet moet worden uitgesloten dat er grotere hoeveelheden gegevens die niet op relevantie zijn onderzocht voor langere tijd beschikbaar blijven, waarmee geen recht wordt gedaan aan het principe van «select while you collect». De Afdeling adviseert in het licht van de Europese rechtspraak, hierop nader in te gaan.
De regering onderkent dat de ontwikkelingen in de Europese rechtspraak in de richting lijken te gaan dat steeds strengere eisen (en waarborgen) worden gesteld aan het vergaren en bewaren van grote hoeveelheden gegevens, waarin ook gegevens zitten van personen die niet onder de aandacht staan van opsporingsinstanties of inlichtingen- en veiligheidsdiensten. Tegelijkertijd moet worden vastgesteld dat het EHRM telkens per voorgelegde casus naar het stelsel als geheel kijkt en de daarin opgenomen waarborgen. Bij de vormgeving van het wetsvoorstel is van deze ontwikkeling kennisgenomen en is – mede naar aanleiding van hetgeen in de PIA Wiv ter zake is gesteld – voorzien in de verplichting om geïntercepteerde communicatie zo snel mogelijk op relevantie te toetsen. Voor zover gegevens worden bewaard is daaromtrent – aan de hand van voorbeelden – uitvoerig uiteengezet waarom dat noodzakelijk is. Waar het gaat om het door Jacobs voorgestelde uitgangspunt wordt met de driefasenaanpak overigens op hoofdlijnen wel degelijk recht gedaan: interceptie en search (gericht op interceptie) zijn nauw met elkaar verweven en ook daarvan is het doel om tot een optimalisatie van het interceptieproces te komen; aan de hand van (technische) filters worden irrelevante gegevens direct uitgefilterd en weggegooid.

f. Vernietiging niet onderzochte gegevens

De bewaartermijn van drie jaar in het kader van onderzoeksopdrachtgerichte interceptie is naar het oordeel van de regering noodzakelijk en proportioneel in een democratische samenleving als bedoeld in artikel 8 lid 2 EVRM. Kenmerkend voor het inlichtingen- en veiligheidsdomein is dat vaak lange tijd onduidelijk is welke exacte betekenis gegevens hebben. Zo werd na de aanslagen in Parijs en Brussel duidelijk dat ISIS al jaren bezig was geweest aanslagplegers naar Europa te sturen. Direct na de aanslagen hebben Europese inlichtingen- en veiligheidsdiensten de gegevens die zij in deze jaren hebben vergaard (nogmaals) uitgekamd op zoek naar verbanden tussen de aanslagplegers en nog onbekende derden. Gegevens die tot dan toe zonder betekenis waren, kregen die in het licht van de aanslagen en hetgeen daaromtrent bekend werd plotseling wel. Enkel omdat deze gegevens konden worden bewaard, konden nieuwe

cellen van ISIS in Europa worden ontdekt en aanslagplots worden verijdeld.

Anders dan bij dataretentie is hierbij geen sprake van het bewaren van alle communicatie (door providers van hun klanten), maar van een verzameling gegevens die binnen de onderzoeksopdracht is vergaard, en die reeds significant is gereduceerd conform de uitleg in paragraaf 3.3.4.4.7.4 van de memorie van toelichting.

Ook andere voorbeelden uit de praktijk, opgenomen in paragraaf 3.3.4.4.7.4 van de memorie van toelichting, wijzen uit dat het onverantwoord is om gegevens die niet kunnen worden geduid te snel te vernietigen. Vanwege het belang een balans te vinden tussen de bescherming van de persoonlijke levenssfeer en de gerechtvaardige eisen van de praktijk, kiest de regering voor de bewaartermijnen zoals aangegeven in de wet. Zoals in paragraaf 10.6 van de memorie van toelichting is aangegeven, sluit dit wetsvoorstel qua bewaartermijnen op hoofdlijnen aan op hetgeen gebruikelijk is in de landen om ons heen.

Gegevens waarvan wordt vastgesteld dat ze niet relevant zijn, worden direct verwijderd en vernietigd.

De regering ziet dan ook geen aanleiding om tot een substantiële verkorting van de bewaartermijn in artikel 48, vijfde lid (47, vijfde lid in het aan de afdeling voorgelegde ontwerp) te komen.

g. Vernietiging niet relevante gegevens

Op grond van artikel 27, eerste lid, worden gegevens verkregen door uitoefening van een bijzondere bevoegdheid zo spoedig mogelijk op hun relevantie voor het onderzoek waarvoor ze zijn verworden onderzocht. Gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel enig ander lopend onderzoek worden vernietigd. Gegevens die, tenzij bij de wet anders is bepaald, na een periode van een jaar niet op hun relevantie voor het onderzoek dan wel enig ander lopend onderzoek zijn onderzocht, worden vernietigd.

De regeling van artikel 27, eerste lid, geldt niet ten aanzien van de uitoefening van de bijzondere bevoegdheid als bedoeld in artikel 48, eerste lid (47, eerste lid, in het aan de afdeling voorgelegde ontwerp). Daar geldt de specifieke regeling van artikel 48, vijfde lid (47, vijfde lid, in het aan de afdeling voorgelegde ontwerp) voor. Ingevolge artikel 48, vijfde lid, mogen gegevens die zijn verzameld door uitoefening van onderzoeksopdrachtgerichte interceptie voor een periode van ten hoogste drie jaren na verwerving worden bewaard ten behoeve van een gegevensverwerking als bedoeld in de artikelen 49 en 50. Gegevens waarvan in dat kader is vastgesteld dat deze niet relevant zijn voor een lopend onderzoek, moeten worden vernietigd. Gegevens die niet op hun relevantie zijn onderzocht, worden na afloop van deze periode vernietigd.

De specifieke bewaartermijn betekent niet dat alle door middel van onderzoeksopdrachtgerichte interceptie vergaarde gegevens gedurende die periode worden bewaard. Dat is niet wenselijk uit oogpunt van privacy en niet wenselijk uit oogpunt van werkbaarheid en efficiency van het proces. Data-reductie is iets dat door alle fases van het interceptieproces heen loopt.

Zo wordt in de eerste fase (verwerving) door middel van technische analyse van de gegevens de uitoefening van de interceptiebevoegdheid geoptimaliseerd. Zoals ook in de memorie van toelichting is verwoord

leidt ook met name het toepassen van filters bij de interceptie ertoe dat de bulk aan gegevens die wordt geïntercepteerd, wordt gereduceerd tot die gegevens die voor verder onderzoek relevant kunnen zijn. Bij filters die gebruikt worden om datastromen te reduceren moet bijvoorbeeld worden gedacht aan het uitfilteren van televisie-uitzendingen, maar ook bijvoorbeeld aan het verwijderen van alle spraakverkeer afkomstig van een satelliet behalve vanuit een bepaald gebied. Met andere woorden het vernietigen van gegevens zal dan ook zeker niet uitzondering zijn.

In de memorie van toelichting is de verhouding tussen beide artikelen verduidelijkt; voorts is artikel 48, vijfde lid, zodanig aangepast dat duidelijk is dat hier een specifieke van artikel 27, eerste lid, afwijkende termijn geldt.

h. Vernietiging versleutelde gegevens

Het advies van de Afdeling heeft aanleiding gegeven om in artikel 48 (artikel 47 in het aan de Afdeling voorgelegde ontwerp) van het wetsvoorstel een afzonderlijke regeling op te nemen in verband met de ontsleuteling van gegevens. In artikel 48, zesde lid, wordt thans voorgesteld om in het geval dat gegevens zijn versleuteld deze gegevens voor een periode van ten hoogste drie jaar na verwerving mogen worden bewaard voor ontsleuteling. Versleutelde gegevens dienen na deze periode te worden vernietigd. De bewaartermijn kan echter – met toestemming van de Minister – telkens met een periode van ten hoogste drie jaar worden verlengd. In de memorie van toelichting is nader uiteengezet wanneer een dergelijke verlenging aan de orde kan zijn. Voor gegevens die zijn ontsleuteld, geldt vervolgens dat deze vanaf dat moment nog voor drie jaar ten behoeve van een verwerking als bedoeld in artikel 49 of 50 van het wetsvoorstel mogen worden aangewend (artikel 48, vijfde lid).

i. Samenwerking buitenland

De Afdeling merkt op dat bij de verstrekking van niet geëvalueerde gegevens aan een dienst waarmee een samenwerkingsrelatie is aangegaan (thans artikel 88, tweede lid, van het wetsvoorstel) er eerst een wegingsnotitie dient te zijn opgesteld (artikel 88 van het wetsvoorstel). Zij stelt voorts vast dat het wetsvoorstel ook een regeling kent waarbij mededeling van ongeëvalueerde gegevens wordt gedaan aan buitenlandse diensten, waarbij niet de eis wordt gesteld dat het gaat om diensten waarmee een samenwerkingsrelatie is aangegaan. Deze constatering van de Afdeling is juist. Bij een verstrekking als bedoeld in het door de Afdeling aangehaalde artikel, dat inmiddels in een afzonderlijk artikel (artikel 64) van het wetsvoorstel is geregeld, is geen sprake van een samenwerkingsrelatie. Het verschil tussen beide regelingen is daarin gelegen, dat het bij de verstrekking op grond van het (nieuw voorgestelde) artikel 64 gaat om een verstrekking die plaatsvindt door de diensten i*n het kader van de goede taakuitvoering van de diensten* en bij de verstrekking in het kader van artikel 89 om een verstrekking *in het kader van een samenwerkingsrelatie*. In dat laatste geval prevaleert het belang van de de samenwerking bij de desbetreffende verstrekking, waarbij uiteraard ook de in artikel 89, eerste lid, van het wetsvoorstel geformuleerde randvoorwaarden in acht genomen moeten worden. De mogelijkheid tot verstrekking van ongeëvalueerde gegevens op grond van artikel 64 is in het wetsvoorstel opgenomen om voor het geval dat zich in de toekomst een situatie van acute noodzaak voordoet, waarbij het noodzakelijk wordt geacht in het kader van een goed taakuitvoering dergelijke gegevens te verstrekken, daartoe ook – gelet op het gesloten verstrekkingstelsel van het wetsvoorstel – een wettelijke grondslag

bestaat. Om aan te geven dat het om uitzonderingsgevallen gaat is daarbij tot uitdrukking gebracht dat er sprake moet zijn van een dringende en gewichtige reden; voorts geldt hier dat door de Minister toestemming moet worden verleend. Hiermee wordt de inbreuk die (mogelijk) op de persoonlijke levenssfeer van burgers wordt gemaakt zoveel mogelijk beperkt. Het eigenstandige karakter van de verstrekkingmogelijkheid ex artikel 64 van het wetsvoorstel, zoals hiervoor toegelicht, brengt met zich mee dat een wettelijk voorgeschreven toets aan de criteria van(thans) artikel 87, derde lid, niet aangewezen wordt geacht. Het voorgaande is in de toelichting op artikel 64 (nieuw) verwerkt.

j. Profilering en geautomatiseerde besluitvorming

Overeenkomstig het advies van de Afdeling is het verbod om uitsluitend op basis van een geautomatiseerde data-analyse maatregelen te bevorderen of te treffen jegens een persoon uitgebreid tot alle vormen van geautomatiseerde data-analyse. De tekst van het wetsvoorstel is daarop aangepast. Voorts is paragraaf 3.5 van de memorie van toelichting met een uitvoerige beschouwing ter zake aangevuld, mede naar aanleiding van de bevindingen en aanbevelingen van de Wetenschappelijke Raad voor het regeringsbeleid (WRR) in haar rapport «Big data» in een vrije en veilige samenleving».

k. Aanpassing technische systemen

Het advies van de Afdeling heeft aanleiding gegeven om paragraaf 3.2.6 van de memorie van toelichting, waar wordt ingegaan op de zorgplichten voor de diensthoofden, nader aan te vullen met argumentatie waarom er naar het oordeel van de regering geen aanleiding bestaat om een bepaling op te nemen inzake *privacy by design* en *by default*. De kern daarvan is, dat de werkwijze van de dienst – waarbij grote hoeveelheden gegevens worden verwerkt waarvan de relevantie voor de taakuitvoering dient te worden vastgesteld, – een gecompliceerd proces is (waarin ook de menselijke component – zoals beoordeling van de relevantie – een plek moet krijgen) en dat deze zich niet louter laat vertalen in in technische systemen in te bouwen waarborgen. Daarnaast wordt opgemerkt dat waar het gaat om het op een privacy-vriendelijke manier inrichten van de informatiesystemen, binnen inlichtingen- en veiligheidsdiensten – juist vanwege de aard van de verwerkte gegevens en de onderkende privacy-gevoeligheid daarvan – er standaard voorzieningen zijn getroffen, zoals ingebouwde autorisatieprocedures; dit naast diverse fysieke, organisatorische en personele beschermingsmaatregelen. De regering ziet geen aanleiding om in het wetsvoorstel alsnog een bepaling als hiervoor bedoeld op te nemen.

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.

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.

5. Conclusie: verenigbaarheid met het EVRM

Op de verschillende onderdelen van het advies van de Afdeling die aan de conclusie ten grondslag liggen is reeds uitvoerig gereageerd.

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.[139] 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.

---

[139] Artikel 141 van het voorstel.

6. Strafrechtelijke handhaving medewerkingsplicht

Overeenkomstig het advies van de Afdeling wordt het stelsel van strafrechtelijke handhaving in het wetsvoorstel gehandhaafd.

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.[140] 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 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.[141] 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.

---

[140] Artikel 35, derde lid, van het voorstel.

[141] Toelichting, paragraaf 9.2.1 Toetskader artikel 8 EVRM, *Voorzienbaarheid: de toestemmingssystematiek.*

7. Vormgeving TIB

De Afdeling geeft aan dat onverminderd hetgeen zij in punt 3 van het advies over de TIB heeft opgemerkt, zij over de vormgeving van de TIB – als deze ingevoerd zou worden – enkele opmerkingen heeft. De adviezen op dit punt zijn overgenomen, zoals hieronder toegelicht.

a. Enkelvoudige of meervoudige samenstelling

Overeenkomstig het advies van de Afdeling is de TIB uitgebreid tot drie (volwaardige) leden die als geheel de toetsing uitvoeren. Het wetsvoorstel en de memorie van toelichting zijn hierop aangepast.

b. Benodigde deskundigheid

Naar aanleiding van het advies van de Afdeling is de samenstelling van de TIB aangepast. In plaats dat alle drie de leden van de TIB dienen te voldoen aan de eis dat zij tenminste zes jaren de functie van rechterlijk ambtenaar met rechtspraak belast als bedoeld in artikel 1, onderdeel c, van de Wet op de rechterlijke organisatie, dienen te hebben vervuld, wordt thans voorgesteld dat tenminste twee van de drie leden, waaronder de voorzitter, aan deze eis dient te voldoen. Aldus wordt de mogelijkheid geopend een lid te benoemen die over de eventueel benodigde technische deskundigheid en inzicht in de veiligheidsrisico's beschikt. Het wetsvoorstel en de memorie van toelichting zijn hierop aangepast.

c. Verantwoording

Overeenkomstig het advies van de Afdeling is aan de TIB de plicht opgelegd om op vergelijkbare wijze als de CTIVD jaarlijks voor 1 mei een openbaar verslag uit te brengen van haar werkzaamheden. De voor de CTIVD geldende regeling is daartoe van overeenkomstige toepassing verklaard. Het wetsvoorstel en de memorie van toelichting zijn hierop van toepassing verklaard.

d. Conclusie

Zoals eerder in reactie op onderdeel 3 van het advies van de Afdeling is aangegeven, wordt voorgesteld de TIB toch in te voeren en overeenkomstig het advies zijn het wetsvoorstel en de memorie van toelichting aangepast.

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.

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

8. Mandaat

Het advies van de Afdeling is overgenomen. Overeenkomstig het advies is bij elke bepaling waarin een toestemmingsvereiste is opgenomen een eigen regeling inzake mandaat opgenomen.

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.[142]

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 ultimum remedium is. De diensten zullen altijd eerst proberen rechtstreeks binnen te dringen in het geautomatiseerde werk van het target zelf.»[143]

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.»[144] *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.*[145]

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.[146] *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*

---

[142] Toelichting, paragraaf 12.2.4
[143] Toelichting, paragraaf 3.3.4.4.6.
[144] Toelichting, paragraaf 3.3.4.4.6.
[145] Toelichting, paragraaf 3.3.4.4.6.
[146] Zie onder meer de artikelen 44, negende lid, 53 en 54 van het voorstel.

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.

9. Binnendringen van een geautomatiseerd werk van een derde

De Afdeling heeft opgemerkt dat de toelichting niet geheel eenduidig lijkt te zijn over de vraag wanneer de bevoegdheid tot het binnendringen via een geautomatiseerd werk van een derde zal worden ingezet. Enerzijds wordt de inzet van deze bevoegdheid als ultimum remedium bestempeld, anderzijds wordt gesteld dat dit in overgrote deel van de gevallen gebeurt. Voorop staat dat de diensten altijd eerst, nadat uiteraard de inzet van lichtere, geheel andere middelen is overwogen, zullen proberen om rechtstreeks binnen te dringen in het geautomatiseerde werk van het target. Indien dit niet mogelijk is kunnen alternatieven worden uitgewerkt, waaronder binnendringen via (een) geautomatiseerd werk van (een) derde(n). Paragraaf 3.3.4.4.6 van de memorie van toelichting is hierop aangepast.

Waar het gaat om het begrip «derde» is in voormelde paragraaf tevens een nadere duiding gegeven. Het gaat in ieder geval om een partij die technisch is te relateren aan het target. Daarbij moet onder andere worden gedacht aan een partij die een netwerk aansluit, een dienst levert, software levert of technische kennis levert. In de meeste gevallen zal die derde dus niet een individuele burger betreffen, maar deze is echter niet daarvan uitgesloten. De mogelijkheid om via het geautomatiseerde werk van een individuele burger binnen te dringen is beperkt tot die gevallen dat er geen alternatieve, minder inbreukmakende manieren van binnendringen voorhanden zijn, die succesvol zijn gebleken. De memorie van toelichting is in voormelde zin aangevuld.

De Afdeling wijst er terecht op dat de bijschrijfmogelijkheid ook van toepassing is op het binnendringen via een derde. In de memorie van toelichting was daaraan nog niet specifiek aandacht besteed; dat is alsnog gebeurd. Daarbij is uiteengezet onder welke specifieke omstandigheden deze bijschrijfmogelijkheid in de praktijk toepassing zal vinden. Opgemerkt wordt dat net als bij het eerste verzoek om toestemming voor binnendringen via een geautomatiseerd werk van een derde reeds uitvoerig aandacht dient te worden besteed aan de technische risico's daarvan. Voorts dient ingevolge artikel 31 van het wetsvoorstel van de uitvoering van de bevoegdheid aantekening te worden gehouden; dus ook indien gebruik wordt gemaakt van de bijschrijfmogelijkheid als hier bedoeld. Naar het oordeel van de regering kan hiermee worden volstaan,

en is het niet noodzakelijk om – zoals de Afdeling voorstelt – te voorzien in een toestemmingverlening per geautomatiseerd werk van een derde. De memorie van toelichting is in voormelde zin aangevuld.

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.

10. Toelichting

Bij de vormgeving van de memorie van toelichting is ervoor gekozen om in het algemeen deel uitvoerig in te gaan op de diverse door het wetsvoorstel bestreken onderwerpen, waarbij onvermijdelijk ook de bespreking van de diverse artikelen is meegenomen. Dat heeft ertoe geleid dat de artikelsgewijze toelichting beperkt van omvang is. Deze keuze is ingegeven door het feit dat het voor een aanzienlijk deel om complexe onderwerpen gaat (vergelijk het onderzoek van communicatie), waarbij een samenhangend betoog in al zijn aspecten aangewezen is geacht. Waar mogelijk is een meer technische toelichting op een artikel naar het artikelsgewijs deel overgeheveld.

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.[147] 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».[148]

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

---

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

148 Artikel 29, vijfde lid, van het voorstel. Dit artikel is overigens gelijkluidend 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).

komt bij dat de voorgestelde toets op de verwerving van communicatie van advocaten ook ruimer is dan die voor journalisten.[149]

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 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.[150] *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.[151]

---

[149] Artikel 29, zesde lid, van het voorstel.

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

[151] 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.

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.

11. Overige opmerkingen

a. Samenhang met het wetsvoorstel bronbescherming in strafzaken

Het advies van de Afdeling is overgenomen. De tekst van het wetsvoorstel en de memorie van toelichting zijn dienovereenkomstig aangepast.

b. Medewerkingsplicht oud-medewerkers

Het advies van de Afdeling is overgenomen.

c. «Mededeling» of «Verstrekking»

In het wetsvoorstel is, in navolging van hetgeen in de huidige wet is bepaald, het begrip «mededeling» gehanteerd. Zoals de Afdeling terecht opmerkt is ook de mededeling een vorm van verstrekking. Het gaat daarbij veelal om op enigerlei wijze door de diensten bewerkte gegevens en niet om de (oorspronkelijke) aan de mededeling ten grondslag liggende gegevens. Overeenkomstig het advies is het gebruik van de term mededeling en verstrekking in het wetsvoorstel en de memorie van toelichting op consistentie nagelopen en waar nodig aangepast.

Van de gelegenheid is gebruik gemaakt om in het wetsvoorstel en de memorie van toelichting enkele redactionele en technische verbeteringen aan te brengen. Voorts is de waar het gaat om de informatieverplichting voor aanbieders van communicatiediensten ter zake van de verstrekking van opgeslagen gegevens en de verstrekking van zogeheten verkeersgegevens de delegatiegrondslag aangepast. De aanvankelijk daarin voorziene differentiatie naar categorieën van communicatiediensten bleek bij nader inzien niet wenselijk. Ook is bij de regeling inzake de bijzondere bevoegdheid tot het verrichten van DNA-onderzoek een maximum bewaartermijn voor DNA-profielen opgenomen; deze is gesteld op 30 jaren. Ook is de in de regeling voor DNA-onderzoek opgenomen delegatiegrondslag opnieuw geformuleerd. Bij de regeling inzake onderzoek van communicatie is naast het (begrip) nummer ook het (begrip) technisch kenmerk opgenomen, dat zowel bij gerichte interceptie als bij het opvragen van verkeers- en gebruikersgegevens van belang kan zijn. In de regeling voor het verlenen van ontslag aan de leden van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten is toegevoegd dat bij het bereiken van de leeftijd van 70 jaar ontslag wordt verleend. Met de totstandkoming en inwerkingtreding van de Wet Huis voor Klokkenluiders was het noodzakelijk om te voorzien in enkele aanpassingen daarvan, indien het voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten 20.. tot wet zal zijn verheven en in werking getreden. Ten slotte zijn er diverse samenloopbepalingen opgenomen in het wetsvoorstel en is de memorie van toelichting hierop aangepast. Het gaat daarbij om de samenloop van het wetsvoorstel met enkele bij het parlement aanhangige wetsvoorstellen, te weten het voorstel van wet open overheid (Kamerstukken 33 328), het voorstel van Rijkswet op het Nederlanderschap in verband met het intrekken van het Nederlanderschap in het belang van de nationale veiligheid (Kamerstukken 34 356), het voorstel van wet houdende regels inzake het beheer, de informatievoorziening, de controle en de verantwoording van de financiën van het Rijk, inzake het beheer van publieke liquide middelen buiten het Rijk en inzake het toezicht op het beheer van publieke liquide middelen buiten het Rijk en publieke financiële middelen buiten het Rijk (Comptabiliteitswet

2016) (Kamerstukken 34 426), het voorstel van wet houdende regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity) (Kamerstukken 34 388) en het voorstel van wet tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken (aanpassing bewaarplicht telecommunicatiegegevens) (Kamerstukken 34 537). Voorts is een overgangsrechtelijke voorziening getroffen voor de leden van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten. Tot slot is voorzien in de mogelijkheid van toepassing van artikel 12 van de Wet raadgevend referendum.

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,
J.P.H. Donner

Ik moge U, mede namens de Minister-President, Minister van Algemene Zaken, de Minister van Defensie en de Minister van Veiligheid en Justitie, verzoeken het hierbij gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk