MEMORIE VAN TOELICHTING

Inhoudsopgave

I Algemeen deel

1. Aanleiding voor het wetsvoorstel
1.1 Inleiding
1.2 De evaluatie van de Wiv 2002
1.3 Voorgeschiedenis wijzigingen van de Wiv 2002
1.4 Een geheel nieuwe wet op de inlichtingen- en veiligheidsdiensten

2 De diensten en de coördinatie tussen de diensten
2.1 Algemeen
2.2 De taken van de diensten
2.3 De sturing van de AIVD en de MIVD
2.4 De coördinatie van de taakuitvoering
2.4.1 De coördinator van de inlichtingen- en veiligheidsdiensten
2.4.2 De Commissie Veiligheids- en Inlichtingendiensten Nederland
2.4.3 De Geïntegreerde Aanwijzing Inlichtingen- en Veiligheidsdiensten
2.5 Bijzondere bepalingen betreffende de functionarissen die ten behoeve van de diensten werkzaam zijn

3 De verwerking van gegevens door de diensten
3.1 Algemeen
3.2 De algemene bepalingen inzake gegevensverwerking
3.3 De verzameling van gegevens
3.3.1 Algemeen
3.3.2 De algemene bevoegdheid van de diensten tot gegevensverzameling
3.3.3 De bijzondere bevoegdheden tot gegevensverzameling van de diensten
3.3.3.1 Algemeen
3.3.3.2 Het toepassingsgebied van de bijzondere bevoegdheden
3.3.3.3 De toestemmingsverlening met betrekking tot de uitoefening van bijzondere bevoegdheden door de diensten
3.3.3.4 Bijzondere bevoegdheden
3.3.3.4.1 Algemeen
3.3.3.4.2 Observeren en volgen
3.3.3.4.3 Agenten
3.3.3.4.4 Onderzoek van besloten plaatsen, van gesloten voorwerpen, aan voorwerpen en DNA-onderzoek
3.3.3.4.5 Openen van brieven en andere geadresseerde zendingen
3.3.3.4.6 Verkennen van en binnendringen in geautomatiseerde werken
3.3.3.4.7 Onderzoek van communicatie
3.3.3.4.7.1 Algemeen
3.3.3.4.7.2 Aanbieders van communicatiediensten
3.3.3.4.7.3 Onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers
3.3.3.4.7.4 Onderzoek van communicatie in andere gevallen
3.3.3.4.7.5 Informatieverzoeken en medewerkingsplicht met betrekking tot telecommunicatiegegevens

3.3.3.4.7.6 Medewerkingsplicht bij ontsleuteling van communicatie
3.3.3.4.8 Toegang tot plaatsen
3.3.3.5 Afwegingskader en verslaglegging
3.3.3.6 Het uitbrengen van verslag omtrent de uitoefening van enkele bijzondere bevoegdheden
3.3.4 Bijzondere bepalingen inzake geautomatiseerde data-analyse
3.3.5 De verstrekking van gegevens
3.3.5.1 Algemeen
3.3.5.2 De interne verstrekking van gegevens
3.3.5.3 De externe verstrekking van gegevens
3.3.5.3.1 Algemene bepalingen
3.3.5.3.2 Bijzondere bepalingen betreffende de externe verstrekking van persoonsgegevens
3.3.6 De verwijdering, vernietiging en overbrenging van gegevens

4 Overige bijzondere bevoegdheden van de diensten
4.1 Algemeen
4.2 De oprichting en inzet van rechtspersonen
4.3 Het bevorderen of treffen van maatregelen

5 Kennisneming van door of ten behoeve van de diensten verwerkte gegevens
5.1 Algemeen
5.2 Recht op kennisneming van persoonsgegevens
5.2.1 Algemeen
5.2.2 Kennisneming van omtrent de aanvrager verwerkte persoonsgegevens
5.2.3 Kennisneming van persoonsgegevens van een overleden echtgenoot, geregistreerd partner, kind of ouder
5.2.4 De wijze van kennisneming van gegevens en het afleggen van een verklaring omtrent door de dienst verwerkte gegevens
5.2.5 Kennisneming van eigen persoonsgegevens door (oud) medewerkers van de diensten
5.3 Het recht op kennisneming van andere gegevens dan persoonsgegevens
5.4 Weigeringsgronden en beperkingen

6 Samenwerking tussen inlichtingen- en veiligheidsdiensten en met andere instanties
6.1 Algemeen
6.2 Samenwerking tussen de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst
6.3 Samenwerking met inlichtingen- en veiligheidsdiensten van andere landen
6.3.1 Algemeen
6.3.2 Het aangaan van en onderhouden van samenwerkingsrelaties met inlichtingen- en veiligheidsdiensten van andere landen
6.3.3 De verstrekking van gegevens alsmede het verlenen van technische en andere vormen van ondersteuning in samenwerkingsrelaties
6.4 De samenwerking van de diensten met andere instanties
6.5 Nadere regels inzake samenwerkingsverbanden

7 Toezicht, klachtbehandeling en de behandeling van meldingen van vermoedens van misstanden
7.1 Algemeen
7.2 Huidig stelsel extern toezicht
7.3 Versterking van het toezichts- en klachtstelsel
7.3.1 Het advies van de commissie Dessens
7.3.2 De uitwerking van het kabinetsstandpunt in het wetsvoorstel
7.4 De behandeling van meldingen inzake vermoedens van misstanden

8 Geheimhouding

9 Grondrechtelijke en mensenrechtelijke aspecten
9.1 Algemeen
9.2 Het recht op eerbiediging van de persoonlijke levenssfeer
9.2.1 Toetsingskader
9.2.2 Het recht op bescherming van persoonsgegevens
9.2.3 Het recht op bescherming van het huisrecht
9.2.4 Het recht op bescherming van het brief-, telefoon- en telegraafgeheim
9.3 Het recht op daadwerkelijk rechtsmiddel

10 Financiële gevolgen voor het Rijk

11 Lasten voor het bedrijfsleven

12 Consultatie, adviezen en privacy impact assessment

II Artikelsgewijze toelichting

Bijlage 1: Transponeringstabel huidige en nieuwe bepalingen

Bijlage 2: Opbouw wetsvoorstel

Bijlage 3: Overzicht bijzondere bevoegdheden en waarborgen

Hoofdstuk 1 Aanleiding wetsvoorstel

1.1 Inleiding

Op 29 mei 2002 is de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) in werking getreden. De Wiv 2002 is sinds zijn inwerkingtreding in zijn algemeenheid een adequaat instrument gebleken voor de AIVD en de MIVD om de aan hen in de Wiv 2002 opgedragen taken te vervullen. Een en ander neemt niet weg dat gaandeweg in de toepassingspraktijk zich kwesties voordeden, waarvoor de Wiv 2002 geen of een niet in alle opzichten toereikend antwoord bleek te geven. In de afgelopen jaren is voorts gebleken dat de wettelijke regeling van de bijzondere bevoegdheden op het vlak van interceptie van communicatie en het onderzoeken van geautomatiseerde werken door de enorme ontwikkelingen in de informatie- en communicatietechnologie sinds de inwerkingtreding van de wet tekort ging schieten en dat het van belang was om te onderzoeken of en, zo ja, welke aanvullende voorzieningen er voor een goede taakuitoefening van de diensten op dat vlak vereist waren. Ook diverse rapporten van de CTIVD gaven aanleiding om te bezien of de wet op onderdelen niet aangepast zou moeten worden.

1.2 De evaluatie van de Wiv 2002

In 2013 is op verzoek van de Tweede Kamer[1] een evaluatie van de Wiv 2002 uitgevoerd. Deze evaluatie is uitgevoerd door de Evaluatiecommissie Wiv 2002, onder voorzitterschap van mr. drs. C.W.M. Dessens (commissie Dessens).[2]

De evaluatiecommissie heeft op 2 december 2013 haar rapport uitgebracht, dat diezelfde dag zowel aan de beide kamers der Staten-Generaal is gezonden als voor het grote publiek openbaar is gemaakt. De evaluatiecommissie komt in haar evaluatierapport in algemene zin tot de conclusie dat de doelstellingen van de wetgever om met de nieuwe wet een formeelwettelijke basis te bieden voor de werkzaamheden van de AIVD en de

[1] Neergelegd in de (gewijzigde) motie Elissen/Çorüz, Kamerstukken II 2011/12, 29 925, nr. 81.
[2] Aan de commissie werd gevraagd in haar onderzoek in ieder geval aandacht te besteden aan de volgende vragen: (a) heeft de wet datgene gebracht wat de wetgever daarmee voor ogen had, (b) is de wet in de praktijk een werkbaar instrument gebleken voor de taakuitvoering van de diensten en (c) welke knel- en aandachtspunten zijn in de toepassingspraktijk van de wet te onderkennen. Bijzondere aandacht werd voorts gevraagd voor een tweetal aspecten, namelijk: (a) zijn de bevoegdheden van de diensten toereikend en voldoen de waarborgen die zijn gesteld. Daarbij zou tevens acht geslagen dienen te worden op huidige en toekomstige ontwikkelingen, zoals op technologisch vlak en op het vlak van cyber, en (b) voldoet het toezicht op de diensten.

MIVD in het belang van de nationale veiligheid, en tegelijk deze werkzaamheden te voorzien van een stevige inbedding in de democratische rechtsstaat, op vele goede manieren in de wet tot uitdrukking zijn gekomen. De commissie wijst er voorts terecht op dat zowel de technologie als de gedachten over - de uitleg van – wettelijke en verdragsrechtelijke normen betreffende de inlichtingen- en veiligheidsdiensten in het laatste decennium een ontwikkeling hebben doorgemaakt. Dat was ook mede de reden om in de onderzoeksopdracht aan de commissie specifiek aandacht voor de technologische ontwikkelingen te vragen, temeer nu ook reeds eerder – vergelijk de rapporten van de CTIVD (onder meer rapport 28[3]) – was geconstateerd dat de wet op dit punt mogelijk achter liep bij de praktijk. Deze technologische ontwikkelingen vragen, aldus de commissie, om een aanpassing van de bevoegdheden van de diensten en tegelijkertijd om een nieuwe balans met de wettelijk geregelde waarborgen en transparantie.

De commissie heeft in haar rapport – gerelateerd aan enkele door haar onderkende thema's – conclusies en aanbevelingen gedaan. Het gaat daarbij naast enkele bevindingen en conclusies van algemene aard, zoals met betrekking tot de taakstelling van de diensten, om bevindingen en conclusies met betrekking tot de sturing (intern en extern) op de werkzaamheden van de diensten, het toezicht op de diensten, de inzet van bijzondere bevoegdheden in de digitale wereld, samenwerking tussen AIVD en MIVD, samenwerking tussen de diensten en andere organisaties alsmede overige waarborgen.

Het kabinet heeft bij brief van 11 maart 2014 zijn reactie op de conclusies en aanbevelingen van de commissie gegeven[4], die in een Algemeen Overleg met de vaste commissie van Binnenlandse Zaken en van Defensie op 16 april 2014 zijn besproken. Het kabinet heeft aangegeven dat het in algemene zin de conclusies en aanbevelingen van de commissie overneemt. Op enkele specifieke onderdelen, zoals bijvoorbeeld met betrekking tot het toezicht door de CTIVD, heeft het kabinet aangegeven te kiezen voor een andere benadering dan waartoe de commissie adviseert. Aansluitend heeft het kabinet op 21 november 2014 nog een aanvullende reactie[5] uitgebracht op het onderdeel bijzondere bevoegdheden in de digitale wereld; dat standpunt is op 10 februari 2015 in een Algemeen Overleg met de eerdergenoemde commissies besproken.

Dit wetsvoorstel bevat de weerslag van hetgeen na de evaluatie van de Wiv 2002 door het kabinet is besloten en besproken met de Tweede Kamer. In het wetsvoorstel zijn voorts ook enkele eerder voorgestelde (niet-controversiële) wijzigingen uit het ingetrokken post-Madridwetsvoorstel opnieuw opgenomen; het voornemen daartoe is

[3] Toezichtsrapport inzake de inzet van Sigint door de MIVD (23 augustus 2011).
[4] Kamerstukken II 2013/14, 33 820, nr. 2.
[5] Kamerstukken II 2013/14, 33 820, nr. 4.

indertijd bij gelegenheid van de intrekking aan beide kamers der Staten-Generaal gemeld.[6] Voorts vloeien enkele wijzigingen voort uit aanbevelingen in door de CTIVD uitgebrachte rapporten in de afgelopen jaren. In de toelichting op de diverse bepalingen zal, waar nodig en relevant, aan een en ander worden gerefereerd.

1.3 Voorgeschiedenis wijzigingen van de Wiv 2002

De Wiv 2002 is in de loop der jaren in tweetal opzicht inhoudelijk gewijzigd. Zo is met ingang van 29 december 2006 aan zowel de AIVD als de MIVD een nieuwe taak toegekend in het kader van de invoering van het nieuwe stelsel voor de beveiliging van personen en voor de bewaking en de beveiliging van objecten en diensten.[7] In het kader van deze taak stellen de diensten (desgevraagd) risico- en dreigingsanalyses op; de nieuwe taak van de MIVD beperkt zich in dit verband overigens tot het opstellen van dreigingsanalyses en voorts alleen voor zover deze ziet op personen, objecten en diensten met een militaire relevantie.[8] Daarnaast is per 10 oktober 2010 – in het kader van de staatkundige herstructurering van het koninkrijk - de Wiv 2002 ook van toepassing verklaard op de openbare lichamen Bonaire, Eustatius en Saba.[9] Daarnaast zijn er in de loop der jaren nog enkele, meer wetstechnische wijzigingen aangebracht, zoals de aanpassing van de artikel 60 en 62 van de Wiv 2002 aan het nieuwe politiebestel.

Voorts is bij Koninklijke boodschap van 15 september 2014 een voorstel van wet tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met de invoering van een onafhankelijke bindende toets voorafgaand aan de inzet van bijzondere bevoegdheden jegens journalisten, welke gericht is op het achterhalen van hun bronnen, bij de Tweede Kamer der Staten-Generaal ingediend.[10] De hierin voorgestelde wijziging van de Wiv 2002 vloeit voort uit een uitspraak van het Europees Hof voor de Rechten van de Mens (EHRM) van 22 november 2012 in een door De Telegraaf c.s. tegen de Staat der Nederlanden aanhangig gemaakte zaak.[11] Het EHRM komt daarin unaniem tot het oordeel dat de inzet van bijzondere bevoegdheden van de AIVD jegens journalisten van De Telegraaf een schending oplevert van artikel 8 en 13 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM). Bij brief van 7 december 2012 heeft de Minister van

[6] Kamerstukken 2010/11, 30 553, nr. 18.
[7] Artikel 6, tweede lid, onder e en artikel 7, tweede lid, onder f, Wiv 2002.
[8] Kamerstukken 28 974.
[9] Wet van 17 mei 2010 tot aanpassing van wetten in verband met de nieuwe staatsrechtelijke positie van Bonaire, Sint Eustatius e Saba als openbaar lichaam binnen Nederland (Aanpassingswet openbare lichamen Bonaire, Sint Eustatius en Saba)(Stb. 2010, 350).
[10] Kamerstukken II 2014/15, 34 027, nrs. 1-4.
[11] EHRM, Telegraaf Media Nederland Landelijke Media B.V. en anderen t. Nederland (No. 39315/06).

Binnenlandse Zaken en Koninkrijksrelaties, mede namens de Minister van Veiligheid en Justitie, de Tweede Kamer der Staten-Generaal geïnformeerd omtrent de gevolgen die aan de uitspraak van het EHRM worden verbonden.[12] Kortheidshalve wordt voor een nadere uiteenzetting ter zake verwezen naar de desbetreffende kamerstukken. De in dit wetsvoorstel voorziene wijziging is in artikel 24, vierde lid, van onderhavig wetsvoorstel verwerkt. Gelet op de stand van zaken van de parlementaire behandeling van dat wetsvoorstel is afgezien van het opnemen van een samenloopbepaling in onderhavig wetsvoorstel.

1.4 Een geheel nieuwe wet op de inlichtingen- en veiligheidsdiensten

Gekozen is voor het opstellen van een voorstel voor een geheel nieuwe wet op de inlichtingen- en veiligheidsdiensten. Het aantal in de huidige wet aan te brengen wijzigingen bleek zodanig omvangrijk dat, conform hetgeen in de Aanwijzingen voor de regelgeving is bepaald, de voorbereiding van een geheel nieuwe wet aangewezen is. Op deze wijze wordt ook de begrijpelijkheid van en het inzicht in de samenhang van de diverse voorstellen gediend.

De keuze voor het opstellen van een geheel nieuwe wet brengt met zich dat in het wetsvoorstel ook diverse bepalingen zijn opgenomen, die ten opzichte van de huidige wet geen wijziging hebben ondergaan. Dat betreft bijvoorbeeld hoofdstuk 1 van de wet waarin een tweetal algemene bepalingen zijn opgenomen en de regeling inzake de kennisneming van door of ten behoeve van de diensten verwerkte gegevens. De toelichting op deze en andere bepalingen, waarbij geen sprake is van een wijziging ten opzichte van de huidige situatie, is algemeen van aard gehouden. Voor een meer gedetailleerde toelichting ter zake wordt verwezen naar hetgeen in het kader van de parlementaire behandeling van de Wiv 2002 is gewisseld.

Diverse in het wetsvoorstel opgenomen bepalingen inzake de verwerking van gegevens, waarbij naast de algemene bevoegdheid tot gegevensverzameling ook bijzondere bevoegdheden ter zake kunnen worden ingezet, maken – in meer of mindere mate – een inbreuk op relevante grond- en mensenrechten, in het bijzonder de artikelen 10, 12 en 13 Grondwet en artikel 8 EVRM. Bij de uitwerking van de verschillende bevoegdheden en andere relevante aspecten van gegevensverwerking (zoals de verstrekking van gegevens) is op de daaruit voortvloeiende eisen acht geslagen, waarbij op een evenwichtige manier recht is gedaan aan zowel het belang van de nationale veiligheid als aan dat van het recht op bescherming van de persoonlijke levenssfeer. In hoofdstuk 9

[12] Kamerstukken II 2012–2013, 30 977, nr. 49.

van deze memorie van toelichting wordt op de verschillende grondrechtelijke en mensenrechtelijke aspecten van het wetsvoorstel ingegaan.

In *bijlage 1* bij deze memorie van toelichting is een transponeringstabel opgenomen, waarin is aangegeven welke bestaande bepalingen in de bepalingen van het wetsvoorstel – geheel of gedeeltelijk, al dan niet aangepast – zijn terug te vinden.

De huidige wet kent een thematische opbouw. De opbouw van het wetsvoorstel sluit daarbij aan. Wel is een extra hoofdstuk, nieuw hoofdstuk 4 (overige bijzondere bevoegdheden van de diensten), ingevoegd. Deze wijziging was reeds voorzien in het ingetrokken post-Madridwetsvoorstel. De achtergrond daarvoor is dat in het hoofdstuk gegevensverwerking ten onrechte enkele bijzondere bevoegdheden (oprichten rechtspersonen en bevorderen en treffen van maatregelen) zijn opgenomen die juist geen betrekking hebben op gegevensverwerking en waarvoor de daarvoor geldende vereisten niet in de volle breedte van toepassing zijn. In *bijlage 2* bij deze memorie van toelichting is de opbouw van het wetsvoorstel weergegeven. In *bijlage 3* is ten slotte een overzicht opgenomen van de bijzondere bevoegdheden en de daarbij van toepassing zijnde voorwaarden c.q. waarborgen.

Hoofdstuk 2 De diensten en de coördinatie tussen de diensten

2.1 Algemeen

Hoofdstuk 2 van het wetsvoorstel geeft, evenals het huidige hoofdstuk 2 van de Wiv 2002, een regeling voor de coördinatie van de taakuitvoering van de diensten, de instelling en taakstelling van de AIVD en MIVD, de verslaglegging omtrent de taakuitvoering van de diensten, enkele bijzondere bepalingen betreffende de functionarissen die ten behoeve van de diensten werkzaam zijn en een delegatiegrondslag voor het bij ministeriële regeling kunnen treffen van nadere regels met betrekking tot organisatie, werkwijze en beheer van de diensten. Ten opzichte van de huidige regeling zijn, ter implementatie van de kabinetsreactie op de aanbevelingen van de commissie Dessens ter zake, enkele wijzigingen aangebracht, die met name betrekking hebben op de rol van de coördinator en de coördinatie van de taakuitvoering. Daarnaast is voorzien in een aanvulling van de taakstelling van de diensten waar het gaat om het uitvoeren van zogeheten naslagen. Deze aanvulling strekt ter uitvoering van een aanbeveling van de CTIVD. Tot slot is voorzien in een bepaling, waarbij de hoofden van de diensten een zorgplicht wordt opgelegd in verband met de beveiliging van de

ambtenaren van de diensten.[13] In het onderstaande zullen de verschillende (inhoudelijke) wijzigingen worden toegelicht.

2.2 De taken van de diensten

De artikelen 6, tweede lid, en 7, tweede lid, van de huidige wet regelen de taakstelling van de AIVD onderscheidenlijk MIVD. Zo is de AIVD als civiele dienst specifiek belast met 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 (de zogeheten a-taak; veiligheidstaak). De MIVD is als militaire dienst specifiek belast met (1) het verrichten van onderzoek omtrent (a) het potentieel en de strijdkrachten van andere mogendheden, ten behoeve van een juiste opbouw en een doeltreffend gebruik van de krijgsmacht, en (b) naar factoren die van invloed zijn of kunnen zijn op de handhaving en bevordering van de internationale rechtsorde voor zover de krijgsmacht daarbij is betrokken of naar verwachting betrokken kan worden, alsmede (2) het verrichten van onderzoek dat nodig is voor het treffen van maatregelen (a) ter voorkoming van activiteiten die ten doel hebben de veiligheid of paraatheid van de krijgsmacht te schaden, (b) ter bevordering van een juist verloop van mobilisatie en concentratie der strijdkrachten en (c) ten behoeve van een ongestoorde voorbereiding en inzet van de krijgsmacht in het kader van de handhaving en bevordering van de internationale rechtsorde (zogeheten a- en c-taak; deels inlichtingen-, deels veiligheidstaak). Deze taken blijven ongewijzigd evenals de aan de beide diensten opgedragen taken in het kader van het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken (Wvo), de beveiliging bevorderende taak alsmede de taak in het kader van het stelsel bewaking en beveiliging.

De taakstelling van de diensten wordt in tweetal opzichten wel gewijzigd. Zo is thans in artikel 6, tweede lid, onder d, en artikel 8, tweede lid, onder e, ter zake van de zogeheten buitenlandtaak (het verrichten van onderzoek naar andere landen) bepaald, dat de onderwerpen waarop dit onderzoek betrekking heeft door de Minister-president, Minister van Algemene Zaken, in overeenstemming met de Ministers van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en van Defensie worden aangewezen. Deze specifieke aanwijzingsgrond komt in het wetsvoorstel te vervallen. In plaats daarvan wordt, zoals ook in de kabinetsreactie op het rapport Dessens is aangegeven, een zogeheten Geïntegreerde Aanwijzing (GA) geïntroduceerd, waarin deze aanwijzing in op gaat. Op de GA zal in het onderstaande nog afzonderlijk worden ingegaan.

[13] Laatstgenoemd voorstel was reeds eerder voorzien in het ingetrokken post-Madridwetsvoorstel.

Een tweede wijziging van de taakstelling van beide diensten betreft een aanvulling daarvan met de taak om het op een daartoe strekkend verzoek van een bij regeling van de Minister-president, Minister van Algemene Zaken, en de Ministers van BZK en van Defensie gezamenlijk aangewezen persoon of instantie doen van mededeling omtrent door de dienst verwerkte gegevens omtrent personen of instanties in bij die regeling aangewezen gevallen; het betreft hier een codificatie van een bestaande praktijk, namelijk het verrichten van zogeheten naslagen. Op dit moment is er namelijk geen specifieke wettelijke grondslag voor het verrichten van een "naslag" door de diensten. Naslag houdt kort gezegd in een zoekslag in de eigen bestanden van de diensten op verzoek van een externe partij om na te gaan of er ten aanzien van een bepaalde persoon of instantie in de dossiers bij de dienst relevante gegevens beschikbaar zijn.[14] Het is dan ook niet aan te merken als een onderzoek in de zin zoals dat in enkele andere taakonderdelen van de diensten is geformuleerd, dus ook geen veiligheidsonderzoek. Het verrichten van naslag wordt tot dusverre als onderdeel van de algemene taak van de diensten beschouwd in het kader van de bescherming van de nationale veiligheid (de artikelen 6 en 7 Wiv 2002). Bij naslag staat namelijk centraal of er vanuit het nationale veiligheidsperspectief een risico bestaat als betrokkene een bepaalde positie gaat bekleden of in een bepaalde omgeving verkeert. In haar toezichtsrapport nr. 36[15] heeft de CTIVD echter de vraag opgeworpen aan welke van de specifieke wettelijke taken van de AIVD genoemd in artikel 6, tweede lid, Wiv 2002 de naslagen kunnen worden gerelateerd. De CTIVD gaf aan dat zij vooralsnog geen antwoord op deze vraag heeft en gaf de betrokken ministers in overweging bij de herziening van de wet aandacht te besteden aan de wettelijke basis van de naslagen en in het bijzonder waar het betreft naslagen naar (kandidaat) politieke ambtsdragers en potentiële leden van de Koninklijke familie. Vast staat volgens de CTIVD wel dat de "integriteit van de openbare sector" een legitiem aandachtsgebied is dat onder het begrip nationale veiligheid valt in de zin van de taakstelling van de dienst.[16] De CTIVD verwijst hiertoe naar de parlementaire behandeling van de huidige wet waaruit blijkt dat het begrip "nationale veiligheid" breed moet worden opgevat en dat hieronder in ieder geval de aandachtsgebieden van (destijds) de Binnenlandse Veiligheidsdienst (BVD) - waar de integriteit van de openbare sector er één van is - begrepen kunnen worden.[17] In het verlengde hiervan kan ook de

[14] Naslag levert gegevens op als de dienst in het verleden in het kader van de uitvoering van zijn taken betrokkene is 'tegengekomen' en over hem of haar bij die gelegenheid informatie is vastgelegd.
[15] CTIVD rapport nr. 36, Vervolgonderzoek naar door de AIVD uitgebrachte ambtsberichten betreffende (kandidaat) politieke ambtsdragers en potentiële leden van de Koninklijke familie.
[16] Zie in dit verband Kamerstukken II 1999/2000, 25 877, nr. 9, p. 14, in combinatie met Kamerstukken II 1999/2000, 25 877, nr. 8, p. 33.
[17] Kamerstukken II 1999/2000, 25 877, nr. 9, p. 14, in combinatie met Kamerstukken II 1999/2000, 25 877, nr. 8, p. 33.

integriteit van het koningshuis onder de taakstelling in algemene zin worden geschaard. De Minister van BZK heeft in zijn reactie op voornoemd rapport toegezegd dit onderwerp mee te nemen bij de herziening van de Wiv 2002.[18] Om redenen van rechtszekerheid, maar ook vanuit het oogpunt van kenbaarheid en voorzienbaarheid richting de betrokkenen - zowel de verzoeker om een naslag als de persoon die het betreft - is er aanleiding gezien om tot een uitgewerkte formeelwettelijke regeling voor naslag te komen. Daarnaast wordt voorgesteld de procedure inzake de naslag (in het bijzonder het verzoek dat aan de verstrekking ten grondslag ligt) nader uit te werken in het nieuwe artikel 50.

Voor de voorgestelde regeling is temeer reden, daar het verrichten van naslag inmiddels een structurele taak is van de diensten. Een belangrijke categorie naslagen in de huidige praktijk van de AIVD is de naslag in de bestanden van de dienst die op verzoek van een externe partij plaatsvindt vanwege een positie waarvoor de betrokkene in aanmerking komt. Het betreft, naast de hiervoor al genoemde naslagen naar (kandidaat) politieke ambtsdragers[19] en potentiële leden van de Koninklijke familie, naslag van kandidaten voor het ambt van Commissaris van de Koning, burgemeester en (waarnemend) rijksvertegenwoordiger of gezaghebber BES. Deze naslagen hebben tot doel bij te dragen bij het verkrijgen van een adequaat beeld inzake eventuele risico’s die samenhangen met de desbetreffende persoon op een bepaalde positie. Inmiddels is de procedure voor deze categorie naslagen in beleid vastgelegd. De CTIVD ziet er op toe dat de wettelijke vereisten bij deze naslagen worden nageleefd.[20]

Daarnaast vindt ook nog in andere dan de hiervoor genoemde gevallen naslag door de diensten plaats, bijvoorbeeld ten behoeve van vitale bedrijven en internationale organisaties. Naslag is in beginsel verbonden aan de voorwaarde dat de belangendrager zelf alle mogelijke middelen voor onderzoek heeft uitgeput en er sprake is van een risico voor de nationale veiligheid. Een aanleiding voor naslag wordt bijvoorbeeld aanwezig geacht wanneer een medewerker bij een vitaal bedrijf op een essentiële maar niet vertrouwensfunctie te werk wordt gesteld en wiens (land van) herkomst onder omstandigheden een risico vormt.

Een plicht voor de diensten om een naslag uit te voeren bestaat er niet. Wel is het zo dat deze in een aantal gevallen sinds jaar en dag standaard wordt uitgevoerd, zoals

---

[18] Kamerstukken II 2013/14, 29 924, nr. 104.
[19] De categorie (kandidaat) politieke ambtsdragers betreft kandidaat-ministers en staatssecretarissen en kandidaat-Kamerleden.
[20] Zie in dit verband de CTIVD toezichtsrapporten nr. 29 en 36.

bijvoorbeeld de naslag van kandidaat-bewindslieden. In andere gevallen waarbij om naslag is verzocht staat de naslag ter discretie van de minister, bijvoorbeeld bij de naslag van kandidaat-Kamerleden. Hoewel naslag geen bijzondere bevoegdheid is van de diensten, is wel sprake van een inbreuk op iemands privacy en dus gelden ook hier de principes van noodzakelijkheid, proportionaliteit en subsidiariteit.

De voorgestelde wettelijke regeling van naslag is als volgt opgezet. Op grond van de artikelen 8, tweede lid, onder f en artikel 10, tweede lid, onder g, worden in een ministeriële regeling de gevallen benoemd waarin naslag naar een persoon of instantie ("het doen van mededeling omtrent door de dienst verwerkte gegevens omtrent een persoon of instantie") kan plaatsvinden en aan wie of welke instanties informatie kan worden verstrekt. Uitgangspunt daarbij is dat naslag beperkt dient te blijven tot een limitatief aantal situaties. Uitsluitend in de gevallen die in de regeling zijn genoemd kan daarom naslag plaatsvinden. Onze betrokken ministers gezamenlijk bepalen in welke gevallen naslag kan plaatsvinden, als waarborg dat naslag slechts kan plaatsvinden in (vooraf) bepaalde gevallen en dat daartoe niet te lichtvaardig wordt besloten. Omdat naslag moet worden beschouwd als een vorm van gegevensverwerking, kan naslag alleen plaatsvinden in de gevallen dat dit noodzakelijk is in het kader van de taakuitvoering van de diensten in het belang van de nationale veiligheid. Binnen dit kader dienen in de ministeriële regeling de gevallen waarin naslag kan plaatsvinden, te worden benoemd.

In het voorgestelde artikel 50 is de procedure voor het verrichten van naslag nader uitgewerkt. Zij voorziet er in de eerste plaats in dat een (schriftelijk) verzoek om naslag moet worden gericht aan de betrokken Minister. Daarnaast is bepaald welke gegevens een dergelijk verzoek in ieder geval moet bevatten. Het verzoek moet in ieder geval bevatten de naam, voornamen, adres en geboortedatum van de betrokken persoon en de aanleiding voor het verzoek. Uitgangspunt is dat degene naar wie een naslag wordt verricht, instemt met het verzoek en dat ter zake een verklaring wordt overgelegd. Alleen in het geval dit de effectiviteit van het uitvoeren van een verzoek zou kunnen schaden, kan op dit uitgangspunt een uitzondering worden gemaakt. Als de naslag relevante (nadelige) gegevens oplevert en besloten wordt degene die om naslag heeft gevraagd daaromtrent te informeren, dan gebeurt dit in beginsel door tussenkomst van de betrokken Minister. Het hoofd van de dienst kan de mededeling namens de Minister doen als dat in de ministeriële regeling uitdrukkelijk mogelijk is gemaakt. In de huidige situatie vindt bijvoorbeeld bij naslag van kandidaat-bewindslieden de mededeling plaats door het hoofd van de dienst.

Met de voorgestelde regeling wordt niet alleen beoogd helderheid te geven over de juridische grondslag voor naslag[21], maar ook over de aard van deze taak. Door naslag als aparte f- en g-taak toe te voegen in onderscheidenlijk de artikelen 8 en 10, is duidelijk dat naslag geen onderzoek is in het kader van de a-taak van de diensten. Naslag moet ook worden onderscheiden van het uit eigen beweging door de dienst uitbrengen van een ambtsbericht naar aanleiding van bevindingen in het kader van een onderzoek van de dienst (artikelen 49, 52 en 53 van het wetsvoorstel).

2.3 De sturing van de AIVD en de MIVD

De commissie Dessens signaleert in haar rapport dat de sturing van de AIVD onderscheidenlijk MIVD door de voor deze diensten verantwoordelijke ministers verschillen in werkwijzen en mandatering. Voorts geeft de commissie aan dat de behoeftestellers en veiligheidspartners beter en eerder zouden moeten worden betrokken bij de voorbereiding van en het opstellen van de jaarplannen en de prioritering van de onderzoeken van de beide diensten. De commissie meent daarnaast dat de aansturing van met name de AIVD voor verbetering vatbaar is. In de kabinetsreactie is ter zake van dit laatste aangegeven dat de aansturing van de AIVD op onderdelen inderdaad dient te worden verstevigd. Dat is gerealiseerd door (verdere) versterking van de rol van de secretaris-generaal en de adviescapaciteit op het departement. De secretaris-generaal ondersteunt met de directeur-generaal van de AIVD de Minister van BZK. Waar het gaat om het door de commissie Dessens geconstateerde verschil in aansturing, wordt opgemerkt dat de organisatorische inbedding van de beide diensten en hun rol binnen de beide departementen verschilt. Overigens is in het wetsvoorstel ten aanzien van verschillende bijzondere bevoegdheden, gelet op de zware inbreuk die daarmee wordt gemaakt op de persoonlijke levenssfeer van personen, de toestemming op het niveau van de minister belegd. Daarmee wordt op wettelijk niveau bestaande verschillen in werkwijzen en mandatering tussen AIVD en MIVD verder verkleind.

2.4 De coördinatie van de taakuitvoering

2.4.1 De coördinator van de inlichtingen- en veiligheidsdiensten

In paragraaf 2.1 van de huidige wet is een regeling opgenomen voor de coördinatie van de taakuitvoering door de diensten, waarbij een centrale rol is weggelegd voor de coördinator. De functie van coördinator wordt al enige tijd vervuld door de secretaris-generaal van het Ministerie van Algemene Zaken. De commissie Dessens heeft in haar

[21] Het verrichten van naslag wordt tot dusverre gebaseerd op het algemene artikel over gegevensverwerking in artikel 12 van de Wiv 2002. Als de naslag (relevante) nadelige gegevens oplevert en besloten wordt deze gegevens in de vorm van een mededeling aan de verzoeker te verstrekken, vormt in beginsel artikel 36 van de Wiv 2002 de basis (ambtsberichten).

rapport aangegeven dat de rol van de coördinator van de inlichtingen- en veiligheidsdiensten onvoldoende uit de verf komt. De commissie wijst daarnaast terecht op de onderscheiden ministeriële verantwoordelijkheid van de betrokken ministers. Wij zijn van mening dat de ministeriële verantwoordelijkheid voor de operationele taakuitvoering zich niet verhoudt met een coördinerende taak van de coördinator op dit terrein. De regering onderschrijft wel de constatering van de commissie dat de rol en taak van de coördinator sterk zijn gekoppeld aan de verantwoordelijkheid van de Minister-president voor de coördinatie en eenheid van het regeringsbeleid op het terrein van nationale veiligheid. De coördinator zal daarom een eigenstandige positie behouden met eenduidig belegde verantwoordelijkheden. Om de coördinator in staat te stellen zijn verantwoordelijkheden in te vullen en zijn taken uit te voeren, wordt deze ondersteund door een secretariaat met gespecialiseerde adviseurs. Een Raadadviseur is tevens de plaatsvervangend coördinator van de inlichtingen- en veiligheidsdiensten.

De taken van de coördinator zijn in artikel 4, derde lid, van het wetsvoorstel, omschreven en komen overeen met hetgeen thans reeds ter zake is bepaald. De eerste taak van de coördinator bestaat uit het voorbereiden van het overleg tussen de betrokken ministers, zoals genoemd in artikel 3, eerste lid, van het wetsvoorstel. In dat artikel is bepaald dat de Minister-president, Minister van Algemene Zaken, en de Ministers van BZK en van Defensie regelmatig onderling overleg voeren over hun beleid betreffende de diensten en de coördinatie van dat beleid. Bij dat overleg kunnen op uitnodiging andere ministers worden betrokken, indien dat, gelet op de door hen te behartigen belangen, noodzakelijk is (artikel 3, derde lid). De tweede taak betreft de coördinatie van de taakuitvoering van de diensten. Voor de uitoefening van deze taken zijn aan de coördinator enkele bevoegdheden toegekend (artikelen 4 tot en met 7 van het wetsvoorstel). Zo zijn de betrokken hoofden van de diensten en de leden van de Commissie Veiligheids- en Inlichtingendiensten Nederland (CVIN-nieuwe stijl) verplicht om alle inlichtingen te verstrekken en medewerking te verlenen die de coördinator voor zijn taak nodig heeft. De coördinator kan voorts besluitvorming afdwingen wanneer dit noodzakelijk is. De coördinator kan daartoe de minister-president voorstellen om het onderwerp in de Raad voor de Inlichtingen- en Veiligheidsdiensten (RIV) te agenderen.

2.4.2 De Commissie Veiligheids- en Inlichtingendiensten Nederland (CVIN)

Anders dan in de huidige wet voorziet het wetsvoorstel in een wettelijke grondslag van wat tot voor kort door het leven ging als het (ambtelijk) Comité Verenigde Inlichtingendiensten Nederland (CVIN), maar nu de Commissie Veiligheids- en Inlichtingendiensten Nederland heet. Met de naamswijziging wordt naar ons oordeel meer recht gedaan aan de huidige situatie, nu er immers nog slechts twee inlichtingen-

en veiligheidsdiensten bestaan. In het verleden bestonden er immers meerdere diensten: de Binnenlandse Veiligheidsdienst (BVD), de Militaire Inlichtingendienst (MID), de Inlichtingendienst Buitenland (IDB) en inlichtingendiensten per krijgsmachtonderdeel. In artikel 5, tweede lid, van het wetsvoorstel is de samenstelling van de commissie geregeld. De commissie bestaat uit vertegenwoordigers van de Ministeries van Algemene Zaken, BZK, Defensie, Buitenlandse Zaken en Veiligheid en Justitie, die daartoe door hun ministers zijn aangewezen. Ook hier geldt dat vertegenwoordigers van andere ministeries kunnen worden uitgenodigd, indien dit, gelet op de door hen te behartigen belangen, noodzakelijk is. Overeenkomstig de aanbeveling van de commissie Dessens zijn in het CVIN thans hoge vertegenwoordigers van het kerndepartement in het CVIN opgenomen, waardoor de betrokkenheid van de departementen is vergroot. Zo is in dit kader medio 2013 het CVIN uitgebreid met de secretaris-generaal van het Ministerie van BZK. Voor het kerndepartement van Defensie is eveneens de secretaris-generaal lid van het CVIN, voor het Ministerie van Veiligheid en Justitie is dat de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en voor het Ministerie van Buitenlandse Zaken de directeur-generaal Politieke Zaken. Voorts zijn de directeur-generaal AIVD en de directeur MIVD lid van het CVIN. De coördinator is voorzitter van de commissie (artikel 5, derde lid).

2.4.3 De Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten

De wettelijke verankering van het CVIN hangt samen met de sterkere positie en meer inhoudelijke rol die deze in de afgelopen jaren heeft gekregen, maar strekt er tevens toe om, overeenkomstig de aanbeveling van de commissie Dessens ter zake, de betrokkenheid van de behoeftestellers en veiligheidspartners bij de voorbereiding en totstandkoming van de prioritering en de jaarplannen van beide diensten wettelijk te borgen. In artikel 5, vierde lid, van het wetsvoorstel is de wijze waarop deze betrokkenheid wordt ingevuld, nader geregeld. Een en ander culmineert in een voorstel voor een Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten (GA), die op grond van artikel 6, eerste lid, uiteindelijk door de Minister-president, Minister van Algemene Zaken, de Minister van BZK en de Minister van Defensie gezamenlijk wordt vastgesteld. Daarmee wordt de werkwijze die eerder gehanteerd werd voor de voorbereiding van het Aanwijzingsbesluit buitenland (zie artikel 6, tweede lid, onder d, en 8, tweede lid, onder e, van de Wiv 2002) voortaan ook van toepassing op de andere taken van de diensten. De behoeftestelling voor beide diensten wordt daarmee over de volle breedte van het takenpakket onderwerp van bespreking en weging in het CVIN en de RIV. Daarmee wordt een goed inzicht in en evenwicht tussen de inlichtingentaak buitenland en de veiligheidstaak van de beide diensten verkregen. Nu deze taken met elkaar verweven zijn, is een goed inzicht voor de betrokken ministers (AZ, BZK, Def, BZ

en VenJ) in de uitvoering van het geheel aan taken van belang om eenduidig sturing kunnen geven bij prioriteits- en besturingsvraagstukken. De Geïntegreerde Aanwijzing zal uiteraard recht blijven doen aan de onderscheiden verantwoordelijkheden van de voor de beide diensten verantwoordelijke ministers. Daartoe behoort de benodigde discretionaire ruimte voor de Ministers van BZK en van Defensie om aanvullend op de in de Geïntegreerde Aanwijzing geformuleerde onderzoeksopdrachten in geval van een acute dreiging of een (potentiële) missie, de onder hen ressorterende diensten daarmee samenhangende onderzoeksopdrachten te kunnen verstrekken. Voorts blijven de diensten ook capaciteit inzetten om ongekende dreigingen te kunnen onderkennen.

De inhoud van de Geïntegreerde Aanwijzing ziet uitsluitend op de in artikel 8, tweede lid, onder a en d, en artikel 10, tweede lid, onder a, c en e, van het wetsvoorstel aan de diensten opgedragen taken. Een aantal taken worden derhalve daarbij buiten beschouwing gelaten. Dit betreffen de zogeheten b-taak van de AIVD en MIVD (veiligheidsonderzoeken), de c-taak van de AIVD en de d-taak van de MIVD (bevorderen van maatregelen ter bescherming van belangen, waaronder de taak van het Nationaal Bureau Verbindingsbeveiliging (NBV)). De reden hiervoor is het specialistische karakter van deze taken. De capaciteit die voor deze taken benodigd is, is niet zonder meer inzetbaar voor de andere taken van de diensten. Ook is bij deze taken sprake van exogene financiering door onder andere de behoeftestellende departementen, die eveneens sturing geven aan de invulling (bijvoorbeeld door de aanwijzing van vertrouwensfuncties en de kostendoorberekening voor de uitvoering van veiligheidsonderzoeken). Daarnaast zijn er nog de e-taak van de AIVD en de vergelijkbare f-taak van de MIVD, waarvoor overigens evenzeer geldt dat onder meer de hiervoor benodigde capaciteit niet zonder meer inzetbaar is voor de andere taken. In het kader van de e-taak van de AIVD en de f–taak van de MIVD gaat het om het opstellen van dreigings- en risico-analyses ten behoeve van de beveiliging van personen, objecten en diensten die daartoe zijn aangewezen, waarbij het voor de MIVD personen, objecten en diensten met een militaire relevantie betreft. Voor deze taken staat de wet de inzet van bijzondere bevoegdheden niet toe. Afgezien van de mogelijkheid om op grond van de algemene bevoegdheid van artikel 17 Wiv 2002 gegevens te verzamelen, zijn de diensten dus aangewezen op de gegevens verkregen uit de andere taken om in de genoemde e- en f-taak te voorzien. De e- en f-taak kunnen niet als zelfstandige (operationele) inlichtingenbehoefte opgenomen worden in de Geïntegreerde Aanwijzing. Vanwege vorenbedoelde samenhang tussen de beschikbaarheid van gegevens voor de e- en f-taak en de andere taken, worden bij de afwegingen met betrekking tot het opstellen en het tussentijds aanpassen van de Geïntegreerde Aanwijzing de mogelijke gevolgen voor de beschikbare informatie voor de uitvoering van de e- en f-taak in ogenschouw genomen.

Het proces van de totstandkoming van de aanwijzing is vastgelegd in artikel 5, vierde lid en artikel 6 van het wetsvoorstel. De Geïntegreerde Aanwijzing zal een periode van vier jaar omvatten en wordt jaarlijks geëvalueerd op actualiteit van de geformuleerde behoeften. De Geïntegreerde Aanwijzing bestaat uit een openbaar deel met toelichting, dat wordt gepubliceerd in de Staatscourant, en een geheim deel met een geheime bijlage. Het geheime deel omvat de basis voor het onderzoek, de samenwerkingsafspraken, waaronder de wijze van (her)prioritering en de uitwerking van de diepgang van de onderzoeken en samenhang met de e- (AIVD) en f-taak (MIVD). De geheime bijlage omvat de onderzoeksthema's en de onderzoeksdoelstellingen die worden toegewezen aan één of beide diensten. De onderzoeksdoelstellingen worden zoveel als mogelijk voor de behoeftestellers voorzien van een gewenste diepgang. Het opstellen van de Geïntegreerde Aanwijzing geschiedt in goed overleg tussen behoeftestellers en de diensten. Het proces start met het geven van inzicht door de beide diensten in de dreigingen met betrekking tot de nationale veiligheid die relevant zijn voor de behoeftestellers.

De coördinator initieert het proces om te komen tot een Geïntegreerde Aanwijzing en de jaarlijkse evaluatie. Dit proces wordt gekoppeld aan de planning & control-cyclus van het Ministerie van BZK en van Defensie en zal elk jaar starten in mei. Onder leiding van de coördinator wordt door een werkgroep van het CVIN een voorstel gemaakt voor de Geïntegreerde Aanwijzing. In artikel 5, vierde lid, onder a en b, zijn de daarvoor vereiste processtappen gedefinieerd. Zo zal jaarlijks de inlichtingenbehoefte van de ministers, bedoeld in artikel 3, eerste en tweede lid, in relatie tot de aan de AIVD onderscheidenlijk MIVD opgedragen taken als bedoeld in artikel 8, tweede lid, onder a en d, onderscheidenlijk artikel 10, tweede lid, onder a, c en in kaart worden gebracht en zal de aldus vastgestelde behoefte aan inlichtingen worden onderworpen aan een proces van weging en prioritering. Dit dient uit te monden in een voorstel voor een Geïntegreerde Aanwijzing ten behoeve van de besluitvorming zoals voorzien in artikel 6 van het wetsvoorstel. De Ministers van BZ en van VenJ zijn dus intensief betrokken bij zowel de opstelling als de weging en prioritering, gericht op een gezamenlijk gedragen Geïntegreerde Aanwijzing. Het voorstel voor een Geïntegreerde Aanwijzing dient, ingevolge artikel 5, vierde lid, onder b, te bestaan uit (a) de onderzoeken die verricht dienen te worden, uitgewerkt naar thema, en de onderzoeksplanning, en (b) de prioritering met betrekking tot de onderzoeken. De uitkomst van dit proces wordt geagendeerd en besproken in het CVIN.

Het voorstel voor de Geïntegreerde Aanwijzing wordt, na afstemming in het CVIN, voorgelegd aan de behoeftestellende Ministers van BZ en van VenJ (artikel 6, derde lid, van het wetsvoorstel). Het voorstel wordt, na de afstemming met deze ministers, ter

instemming voorgelegd aan de Minister-president, Minister van Algemene Zaken, en de Ministers van BZK en van Defensie in verband met agendering in de RIV. Na de instemming van de RIV en vaststelling van de conclusies van de RIV in de Ministerraad, wordt de Geïntegreerde Aanwijzing op grond van artikel 6, eerste lid, formeel vastgesteld door de Minister-president, Minister van Algemene Zaken, Minister van BZK en Minister van Defensie gezamenlijk. Het openbare deel van de Geïntegreerde Aanwijzing wordt gepubliceerd (geldingsduur is 4 jaar). Het openbare en het geheime deel wordt in afschrift toegezonden aan de behoeftestellende ministers. Na de jaarlijkse evaluatie wordt het opnieuw vastgestelde geheime deel eveneens in afschrift toegezonden aan de behoeftestellende ministers.

De Ministers van BZK en van Defensie werken de Geïntegreerde Aanwijzing uit in de jaarplannen (onderzoeksplannen) voor de AIVD onderscheidenlijk MIVD. De jaarplannen worden aan het CVIN en de RIV voorgelegd voor instemming.

Ten minste elke vier maanden wordt onder leiding van de coördinator de voortgang van de uitvoering van de Geïntegreerde Aanwijzing besproken in het CVIN (artikel 5, vierde lid, onder c, van het wetsvoorstel). Indien een tussentijds veranderende dreiging of risico dit noodzakelijk maakt en een mogelijke (her)prioritering aan de orde is, wordt dit zo spoedig mogelijk onder leiding van de coördinator met de beide diensten en vertegenwoordigers van BZK, Defensie, Buitenlandse Zaken en Veiligheid en Justitie besproken. De hiervoor geschetste procedure is daarbij onverkort van toepassing.

2.5 Bijzondere bepalingen betreffende de functionarissen die ten behoeve van de diensten werkzaam zijn

In paragraaf 2.5 van het wetsvoorstel zijn, evenals in de huidige wet reeds het geval is, enkele bijzondere bepalingen opgenomen betreffende de functionarissen die ten behoeve van de diensten werkzaam zijn. In de artikelen 13 (geen opsporingsbevoegdheid) en 14 (reis- en verblijfsverbod risicolanden), die corresponderen met de huidige artikelen 9 en 10, is voorzien in een beperkte inhoudelijke wijziging als gevolg van het feit dat in artikel 80 van het wetsvoorstel thans wordt voorzien in de mogelijkheid dat ambtenaren van de Koninklijke marechaussee (KMar) onder verantwoordelijkheid van de Minister van Defensie en op aanwijzing van het hoofd van de MIVD werkzaamheden voor de MIVD kunnen gaan verrichten. Als gevolg daarvan dienen zij onder reikwijdte van beide bepalingen te worden gebracht.

Ten opzichte van de regeling in de huidige wet is in het wetsvoorstel voorzien in een aanvullende bepaling, te weten artikel 15. Artikel 15 geeft een specifieke regeling in verband met te treffen voorzieningen ter beveiliging van de ambtenaren die werkzaam

zijn bij of ten behoeve van de diensten.[22] De noodzaak van een expliciete regeling is in de afgelopen jaren toegenomen. Ook inlichtingen- en veiligheidsdiensten kunnen een mogelijk doelwit van terroristische aanslagen zijn, hetgeen in het recente verleden uit toen ter beschikking gekomen informatie is gebleken. Dit gegeven heeft onmiskenbaar invloed op het veiligheidsgevoel van de ambtenaren die werkzaam zijn bij of ten behoeve de diensten, zeker in situaties dat zij in het kader van hun taakuitvoering in de operationele sfeer diverse soorten activiteiten dienen te verrichten, waarbij zij een verhoogd veiligheidsrisico lopen. Om dergelijke risico's te minimaliseren worden door de diensten in de praktijk uiteraard al diverse soorten voorzieningen getroffen, waarop om evidente redenen niet in detail kan worden ingegaan. Maar gedacht kan bijvoorbeeld worden aan maatregelen welke strekken ter afscherming van de werkelijke identiteit van operationele medewerkers in relatie tot de functie die zij uitvoeren. Het is wenselijk om in meer algemene zin een juridische basis te scheppen waarop dergelijke voorzieningen zijn terug te herleiden en die tevens uitdrukking geeft aan de zorgplicht die op de hoofden van de diensten als werk- of opdrachtgever rust (artikel 15, eerste lid). Weliswaar legt artikel 15 van de huidige wet aan de hoofden van de dienst de plicht op om te zorgen voor de veiligheid van de personen met wier medewerking gegevens worden verzameld, doch deze verplichting staat in het teken van de gegevensverwerking van de diensten, in het bijzonder de plicht tot bronbescherming. De zorgplicht die in artikel 15, eerste lid, is neergelegd heeft een andere invalshoek: namelijk de zorg voor de veiligheid van het eigen personeel.

Daarnaast is het wenselijk om ten behoeve van een specifieke categorie maatregelen – evenals dat bij de regeling van agenten het geval is – te voorzien in de mogelijkheid om ten behoeve van de personen die het betreft de medewerking van verschillende bestuursorganen te verzekeren, opdat op adequate wijze kan worden voorzien in een door deze personen – voor de taakuitvoering noodzakelijk te achten – aan te nemen identiteit en hoedanigheid. Artikel 15, tweede lid, verklaart daartoe artikel 26, tweede lid, van overeenkomstige toepassing. Het opereren onder een aangenomen identiteit en hoedanigheid door ambtenaren werkzaam bij of ten behoeve van de diensten is overigens alleen toegestaan, indien het hoofd van de dienst daarvoor toestemming heeft verleend. Daarbij moet onder meer worden gedacht aan personen die als operationeel medewerker optreden of deel uitmaken van volg- en observatieteams. In artikel 15, derde lid, wordt voorzien in de verplichting om van de toepassing van het artikel aantekening te houden. Dat biedt de mogelijkheid om omtrent de toepassing van deze bevoegdheid verantwoording af te kunnen leggen (bijvoorbeeld aan de minister of in het kader van een onderzoek van de CTIVD).

[22] Deze regeling was ook opgenomen in het ingetrokken post-Madridwetsvoorstel.

Waar het gaat om meer algemene voorzieningen, die bijvoorbeeld in beginsel alle personen werkzaam bij of ten behoeve van de diensten betreffen, zal volstaan kunnen worden met opneming van deze maatregelen als onderdeel van de beschrijving van de interne organisatie. Waar het echter gaat om specifieke voorzieningen met betrekking tot individuele personen, zoals die waarin het tweede lid voorziet, ligt een specifieke aantekening op persoonsniveau voor de hand.

Tot slot is in artikel 15, vierde lid, bepaald dat het artikel van overeenkomstige toepassing is op de krachtens artikel 79, tweede lid, en 80, tweede lid, aangewezen ambtenaren. Indien deze ambtenaren werkzaamheden verrichten voor de AIVD onderscheidenlijk de MIVD doen zij dat onder verantwoordelijkheid van de Minister van BZK onderscheidenlijk de Minister van Defensie en overeenkomstig de aanwijzingen van het directeur-generaal van de AIVD onderscheidenlijk de directeur van de MIVD. Het is evident dat ook in die situatie de in artikel 15 tot uitdrukking gebrachte zorgplicht toepassing dient te vinden.

Hoofdstuk 3 De verwerking van gegevens door de diensten

3.1 Algemeen

Hoofdstuk 3 van het wetsvoorstel geeft, evenals het huidige hoofdstuk 3 van de Wiv 2002, een (vrijwel) uitputtende regeling voor de kernactiviteit van de inlichtingen- en veiligheidsdiensten, te weten de verwerking van gegevens. Inlichtingenwerk is immers in zijn essentie gegevensverwerking. Hoofdstuk 3 van het wetsvoorstel volgt de structuur en indeling van de huidige regeling, zij het dat de paragraaf inzake bijzondere bevoegdheden van de diensten (3.2.2) in het bijzonder als gevolg van de nieuwe regeling inzake onderzoek van communicatie, in subparagrafen is onderverdeeld. Voorts is er een nieuwe paragraaf met bijzondere bepalingen inzake geautomatiseerde data-analyse ingevoegd (3.3). In bijlage 2 bij deze memorie van toelichting is (onder meer) de structuur en indeling van het nieuwe hoofdstuk 3 weergegeven. Inhoudelijk is de regeling inzake de verwerking van gegevens door de diensten op diverse onderdelen ingrijpend gewijzigd, met name waar het gaat om de bijzondere bevoegdheden van de diensten. Daarop zal in het onderstaande nog uitvoerig worden ingegaan. In bijlage 3 bij deze memorie van toelichting is een overzicht van de bijzondere bevoegdheden opgenomen, waarbij ook is aangegeven welke waarborgen daarbij gelden (toestemmingsniveau, toestemmingsduur, toetsingscriteria e.d.). De regeling inzake verstrekking van gegevens is inhoudelijk ook grotendeels ongewijzigd gebleven; naast een aantal wetstechnische aanpassingen van de bestaande regeling, is met name voorzien in een specifieke regeling ter zake van de verstrekking van gegevens in het kader van een zogeheten naslag en in een regeling voor de verstrekking van ongeëvalueerde gegevens.

In het onderstaande zal thans op de diverse aspecten van de voorgestelde regeling worden ingegaan.

3.2 De algemene bepalingen inzake gegevensverwerking

In paragraaf 3.1 (de artikelen 17 tot en met 21) van het wetsvoorstel zijn enkele bepalingen opgenomen die in algemene zin van toepassing zijn op de verwerking van gegevens door de diensten; deze bepalingen corresponderen met de huidige artikelen 12 tot en met 16 maar zijn op onderdelen aangepast. Onder gegevens worden hier zowel persoonsgegevens als andere gegevens verstaan (artikel 1, aanhef en onder d).

In artikel 17, eerste lid, is in algemene zin de bevoegdheid voor de diensten om gegevens te verwerken neergelegd. De verwerking van gegevens door de diensten dient primair gerelateerd te zijn aan de uitvoering van de aan hen opgedragen taken en de daaraan gerelateerde beheersfuncties (zoals personeels- en salarisadministraties). Daarbij dienen de eisen die bij of krachtens de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) of de Wvo daaraan worden gesteld in acht te worden genomen. Dat betekent bijvoorbeeld dat ingeval gegevens worden verzameld met uitoefening van bijzondere bevoegdheden, de aan de uitoefening daarvan gestelde eisen dient te worden voldaan. Aan de gegevensverwerking worden in artikel 17, tweede tot en met vierde lid, een aantal eisen gesteld. De verwerking van gegevens vindt slechts voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van de Wiv of de Wvo. Deze eis, in het bijzonder de gerichtheid op een bepaald doel, raakt de concrete taakuitvoering door de diensten. De verwerking dient in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze plaats te vinden. Dit zijn eisen die in algemene zin in privacywetgeving aan de verwerking van persoonsgegevens worden gesteld. Waar het gaat om gegevensverwerking door de inlichtingen- en veiligheidsdiensten is in het vierde lid als algemene eis toegevoegd, dat de gegevens die in het kader van de taakuitvoering van de diensten worden verwerkt dienen te zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend. De diensten kunnen in het kader van hun taakuitvoering gegevens verzamelen uit allerlei bronnen (open en gesloten, technisch en menselijk enz.). Gelet op het gebruik van deze gegevens kan worden gemaakt – bijvoorbeeld als basis voor een mededeling als bedoeld in artikel 49 jo. 54 van het wetsvoorstel) – en de gevolgen die dat kan hebben voor personen of organisaties waarop die gegevens betrekking hebben, is het van belang dat expliciet wordt vastgesteld wat de kwaliteit van die gegevens is.

Artikel 18 beschrijft limitatief de kring van personen waaromtrent door de diensten gegevens verwerkt mogen worden. Daarbij is in het eerste en tweede lid onderscheid

gemaakt tussen de beide diensten (AIVD onderscheidenlijk MIVD), hetgeen voortvloeit uit het verschil in taakstelling van beide diensten. Bij de beschrijving van de kring van personen is daarbij aangesloten. Ten opzichte van de huidige regeling is voor beide diensten daaraan toegevoegd, dat ze ook gegevens mogen verwerken van personen omtrent wie dat noodzakelijk is in het kader van het doen van een mededeling als bedoeld in artikel 8, tweede lid, onderdeel f (naslag door de AIVD) onderscheidenlijk artikel 10, tweede lid, onder g (naslag door de MIVD). In artikel 18, derde en vierde lid, is een regeling opgenomen voor de verwerking van gevoelige persoonsgegevens; daaronder worden in dit kader verstaan: gegevens betreffende iemands godsdienst of levensovertuiging, ras, gezondheid en seksuele leven. Het verwerken van deze gegevens enkel en alleen vanwege het feit dat iemand aan een van deze kenmerken voldoet is ingevolge het derde lid niet toegestaan. Dergelijke gegevens mogen alleen plaatsvinden in aanvulling op de verwerking van andere gegevens en voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is (vierde lid). Met het begrip "onvermijdelijk" wordt beoogd aan te geven dat bij de verwerking van een gegeven als hier bedoeld aan een zwaarder criterium dient te worden voldaan, dan aan het in artikel 17, tweede lid, neergelegde noodzakelijkheidscriterium.[23] Over het algemeen wordt politieke gezindheid ook als een gevoelig gegeven beschouwd, maar deze is in zowel de huidige als voorgestelde regeling om evidente redenen van de toepasselijkheid van het derde en vierde lid uitgezonderd. Bij de beoordeling of iemand een gevaar kan vormen voor de democratische rechtsorde, de veiligheid of paraatheid van de Nederlandse krijgsmacht of voor andere in de wet genoemde gewichtige belangen kan immers de vraag naar iemands politieke gezindheid, naast andere aspecten niet buiten beschouwing blijven. Uiteraard moet bij het vastleggen van dit gegeven wel voldaan worden aan de algemene eis ex artikel 17, tweede lid, dat het noodzakelijk is voor een goede uitvoering van de Wiv of de Wvo. Ten opzichte van de huidige regeling in artikel 13 Wiv 2002 is een nieuw artikellid toegevoegd (vijfde lid). Daarin is bepaald dat onverminderd de verwerking van persoonsgegevens als bedoeld in het eerste en tweede lid, de diensten bevoegd zijn tot verwerking van gegevens omtrent andere personen, indien die gegevens en logisch en onlosmakelijk onderdeel vormen van de door de diensten te verwerven of verworven gegevensbestanden. Over het algemeen zullen bij de verwerving van gegevensbestanden (als onvermijdelijk en inherent onderdeel van het gegevensbestand) ook gegevens worden verworven van personen die vanuit de taakstelling van de dienst geen aandacht hebben. De wettelijke basis tot nu toe wordt gezocht in artikel 18, eerste lid, onder e, en

[23] In het kader van de parlementaire behandeling van de Wiv 2002 werd als voorbeeld gegeven, dat het onvermijdelijk zal zijn om bijvoorbeeld de godsdienstige of levensovertuiging van personen of organisaties vast te leggen in de gevallen dat antidemocratische, staatsgevaarlijke of antimilitaristische activiteiten worden ontplooid waarbij de daders hun godsdienstige overtuiging als motief aanvoeren voor hun activiteiten. Zie Kamerstukken II 1997/98, 25 877, nr. 3, p. 20.

tweede lid, onder e: personen wier gegevens noodzakelijk zijn ter ondersteuning van een goede taakuitvoering door de dienst. Voor zover er twijfel zou kunnen ontstaan over de geoorloofdheid van de verwerking van dergelijke persoonsgegevens is ervoor gekozen om dit afzonderlijk te regelen. Dat komt de rechtszekerheid ten goede.

In artikel 19, eerste lid, van het wetsvoorstel wordt, vergelijkbaar met het huidige artikel 14, de (algemene) bevoegdheid tot gegevensverwerking almede de algemene en bijzondere eisen die daaraan worden gesteld ook van toepassing verklaard op de ambtenaren die ingevolge artikel 79 onderscheidenlijk 80 van het wetsvoorstel werkzaamheden verrichten ten behoeve van de AIVD onderscheidenlijk de MIVD. Bij de verwerking van gegevens door deze ambtenaren ten behoeve van de AIVD onderscheidenlijk MIVD dient voorkomen te worden dat die verwerking op enigerlei wordt vermengd met de verwerking van gegevens door deze ambtenaren ten behoeve van andere doeleinden (artikel 18, tweede lid, eerste volzin). Dat is niet alleen noodzakelijk om als voor de desbetreffende dienst verantwoordelijke minister de verantwoordelijkheid voor die gegevensverwerking (ten behoeve van AIVD onderscheidenlijk MIVD) te kunnen dragen, maar ook om de toepasselijkheid en toepasbaarheid van de specifieke normen die voor de gegevensverwerking door of ten behoeve van de diensten gelden te garanderen. Aan het hoofd van de dienst is ten slotte de bevoegdheid gegeven om omtrent de gegevensverwerking aanwijzingen te geven, bijvoorbeeld over de wijze waarop door de hier bedoelde ambtenaren de gegevensverwerking ingericht dient te worden teneinde de vermenging met andere gegevensverwerkingen te voorkomen. In artikel 19, derde lid, wordt de Minister van BZK onderscheidenlijk de Minister van Defensie aangewezen als zorgdrager voor de bij de artikel 79 onderscheidenlijk 80 berustende archiefbescheiden, voor zover die nog niet naar een rijksarchiefbewaarplaats zijn overgedragen.

In de artikelen 20 en 21 wordt aan de hoofden van de diensten enkele zorgplichten opgelegd; deze verplichtingen komen geheel overeen met hetgeen thans in de artikelen 15 en 16 van de Wiv 2002 is geregeld. Deze zorgverplichtingen zullen in de praktijk met name hun uitwerking dienen te krijgen in concrete maatregelen op het vlak van de (inrichting van de) organisatie, het personeel en de invulling van de aan de gegevensverwerking gerelateerde werkprocessen. De in artikel 20 neergelegde zorgplicht van het hoofd van de dienst ziet op de geheimhouding van (a) daarvoor in aanmerking komende gegevens, (b) de geheimhouding van daarvoor in aanmerking komende bronnen waaruit gegevens afkomstig zijn en (c) de veiligheid van de personen met wier medewerking gegevens worden verzameld. Met de onder b geformuleerde zorgplicht wordt beoogd tot uitdrukking te brengen dat de plicht tot bronbescherming niet verder strekt dan strikt noodzakelijk is. Indien gegevens door de dienst uit open bronnen zijn

verkregen en daaraan ontleende gegevens worden (verder) verstrekt, dan stuit vermelding van die bron niet op bezwaren. Waar het gaat om de in artikel 21 neergelegde zorgverplichtingen betreft, wordt met betrekking tot onderdeel c ("de aanwijzing van personen die bij uitsluiting van anderen bevoegd zijn tot de bij de aanwijzing vermelde werkzaamheden in het kader van de verwerking van gegevens") opgemerkt, dat – mede ter uitvoering van het kabinetsstandpunt met betrekking tot het onderdeel "Inzet van bijzondere bevoegdheden in de digitale wereld"[24] – in de regeling van een aantal bijzondere bevoegdheden op het vlak van interceptie een vergelijkbare bepaling is opgenomen (zie de artikelen 33, vierde lid, 34, vijfde lid, en 35, vijfde lid, van het wetsvoorstel). In het kader van de aldaar voorziene vormen van gegevensverwerking dient dus in ieder geval een aanwijzing als hier bedoeld plaats te vinden.

3.3 De verzameling van gegevens

3.3.1 Algemeen

Paragraaf 3.2 van het wetsvoorstel geeft een regeling voor de verzameling van gegevens door de diensten. Allereerst wordt de algemene bevoegdheid tot gegevensverzameling geregeld (artikel 22) en aansluitend worden regels gegeven voor de verzameling van gegevens door uitoefening van bijzondere bevoegdheden. Met betrekking tot de bijzondere bevoegdheden worden diverse aspecten geregeld. In paragraaf 3.2.2.1 worden een tweetal algemene bepalingen inzake de uitoefening van de bijzondere bevoegdheden geformuleerd, te weten inzake het toepassingsbereik van de bijzondere bevoegdheden (artikel 23) en het toestemmingsregime (24). Aansluitend worden in de artikelen 25 tot en met 42 de diverse bijzondere bevoegdheden – voor zover deze gericht zijn op gegevensverwerking dan wel daar ondersteunend aan zijn – geregeld. In paragraaf 3.2.2.9 (artikelen 43 en 44) zijn evenals nu het afwegingskader en de verslagleggingsplicht bij de uitoefening van bijzondere bevoegdheden neergelegd; hierin hebben zich ten opzichte van de huidige regeling (artikelen 32 en 33) geen wijzigingen voorgedaan. Tot slot voorziet paragraaf 3.2.3 in de regeling voor het uitbrengen van een verslag omtrent de uitoefening van enkele bijzondere bevoegdheden, de zogeheten notificatieplicht. De reikwijdte van deze plicht - zie ook hierna – is als gevolg van de voorgestelde wijzigingen in de bijzondere bevoegdheden die betrekking hebben op het onderzoeken van communicatie aangepast.

3.3.2 De algemene bevoegdheid van de diensten tot gegevensverzameling

[24] Zie de brief van de Ministers van BZK en van Defensie van 21 november 2014 (Kamerstukken II 2014/15, 33 820, nr. 4, blz. 3 e.v.), paragraaf 3a, waarin wordt aangegeven dat in de wet ook zal worden voorzien in een (gecombineerd) stelsel van functie- en taakscheiding c.q. compartimentering waar het gaat om toegang tot de gegevens in de verschillende fasen en buiten het interceptieproces.

Artikel 22 van het wetsvoorstel regelt evenals het huidige artikel 17 Wiv 2002 de *algemene* bevoegdheid van de diensten om bij de uitvoering van hun taak, dan wel ter ondersteuning van een goede taakuitvoering, zich voor het verzamelen van gegevens te wenden tot bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken; kort gezegd kan de dienst zich tot een ieder wenden met een verzoek om gegevens. De toepassing van deze bevoegdheid is onderworpen aan de algemene bepalingen inzake gegevensverwerking, zoals hiervoor reeds besproken. Dat betekent dus onder maar dat een verzoek om gegevens altijd plaats dient te vinden voor een bepaald doel, op een zorgvuldige en behoorlijke wijze plaatsvindt en in overeenstemming met de wet dient te zijn. Het willekeurig opvragen van gegevens is dus niet geoorloofd.

In het huidige artikel 17, eerste lid, wordt naast de hiervoor genoemde categorieën van personen en instanties waaraan een verzoek kan worden gericht, ook expliciet de ”verantwoordelijke voor een gegevensverwerking” benoemd (artikel 17, eerste lid, aanhef en onder b). De reden daarvoor was in het bijzonder daarin gelegen, dat in artikel 17, derde lid, Wiv 2002 ter zake is bepaald dat de voor een verantwoordelijke voor een gegevensverwerking geldende wettelijke regels niet van toepassing zijn indien men op grond van het eerste lid (desgevraagd) aan de diensten gegevens verstrekt. Voorts geldt op grond van artikel 17, tweede lid, Wiv 2002 een legitimatieplicht voor de medewerker van de dienst die zich tot een verantwoordelijke wendt met een verzoek om gegevens. De noodzaak voor een afzonderlijke vermelding van de verantwoordelijke voor een gegevensverwerking in het eerste lid, zoals thans wel het geval is, ontbreekt echter; een ieder kan immers – onder omstandigheden – *tevens* verantwoordelijke voor de gegevensverwerking zijn. Er is geen sprake van een nevengeschikte categorie. Waar het primair om gaat is dat de in het huidige artikel 17, derde lid, opgenomen regeling in dat geval van toepassing is en dat kan ook anderszins worden verzekerd; zie daartoe het voorgestelde artikel 22, vierde lid.

Artikel 17, derde lid, Wiv 2002 – en daarmee ook het voorgestelde artikel 22, vierde lid – is van cruciale betekenis voor de uitoefening van de in het eerste lid neergelegde bevoegdheid. Gegevens – zowel persoonsgegevens als andere gegevens – worden door personen en instanties in het algemeen verwerkt voor andere doeleinden dan waarvoor de diensten deze (willen) verwerken. De voor de verwerking van die gegevens toepasselijke wet- en regelgeving, waarin ook het doel voor de verwerking is gespecificeerd, zal er over het algemeen niet in voorzien dat die gegevens door die personen of instanties – in dat kader aangemerkt als de verantwoordelijke voor die

verwerking - ook aan inlichtingen- en veiligheidsdiensten kunnen worden verstrekt.[25] Voor de gevallen waarin niet expliciet in de mogelijkheid van verstrekking is voorzien, dient derhalve een voorziening voorhanden te zijn die garandeert dat als de verantwoordelijke voor een gegevensverwerking besluit om – in weerwil van de ter zake geldende wettelijke voorschriften – toch te verstrekken, de desbetreffende wettelijke voorschriften buiten toepassing worden verklaard. Zoals bij de parlementaire behandeling van het huidige artikel 17, derde lid, reeds is aangegeven, heeft de toepassing van deze bepaling ook andere gevolgen. Verplichtingen voor de desbetreffende verantwoordelijke voor de gegevensverwerking om van gedane verstrekkingen aan de diensten aantekening te houden (protocolplicht) blijven buiten toepassing alsmede – in samenhang daarmee – de verplichting om in het kader van een inzageverzoek van de betrokken persoon deze te informeren omtrent een verstrekking aan een van de diensten; het is evident dat dit laatste aan de effectiviteit van een goede – en veelal heimelijke - taakuitvoering van de diensten in de weg kan staan. Een ander belangrijk gevolg is, is dat ook de verplichting om aan een toezichthouder op de gegevensverwerking door de verantwoordelijke – zoals bijvoorbeeld het College bescherming persoonsgegevens (Cbp) – in het kader van diens controlerende taak informatie te verstrekken over eventuele gegevensverstrekkingen aan de diensten, buiten toepassing blijft. Dat betekent niet dat er geheel geen toezicht op die gegevensverstrekkingen plaatsvindt. Dit toezicht wordt echter uitgeoefend door de CTIVD, die belast is met onder meer het toezicht op de rechtmatige uitoefening van de Wiv 2002 en daarmee dus ook op de toepassing van artikel 17 Wiv 2002. Daarin komt met dit wetsvoorstel geen verandering. Zoals hiervoor al kort aangeduid, voorziet artikel 22, tweede lid, van het wetsvoorstel (evenals artikel 17, tweede lid, Wiv 2002) in een legitimatieplicht voor de dienstmedewerker die zich tot een verantwoordelijke voor de gegevensverwerking wendt. De reden daarvoor is, dat de verantwoordelijke - voordat deze ingaat op om een verzoek voor gegevensverstrekking - zich kan vergewissen dat het verzoek rechtens wordt gedaan door een dienst en dat voor hem – indien hij tot medewerking aan het verzoek besluit – de in artikel 22, vierde lid, neergelegde voorziening van toepassing is.

Ten opzichte van de huidige wettelijke regeling voorziet artikel 22 in twee aanvullingen. Allereerst wordt in artikel 22, derde lid, bepaald dat aan een verzoek om gegevensverstrekking kan worden voldaan door het verlenen van rechtstreeks

[25] Hierop bestaan overigens – in toenemende mate - uitzonderingen. Met name in wetgeving die de gegevensverwerking door overheidsinstanties reguleert, ziet men dat er vaker ook de verstrekking aan de diensten in het kader van de uitvoering van de Wiv 2002 als expliciet mogelijkheid wordt benoemd. Vergelijk onder meer de Wet politiegegevens, de Wet basisregistratie personen, de Wet justitiële en strafvorderlijke gegevens.

geautomatiseerde toegang tot de desbetreffende gegevens dan wel door het verstrekken van geautomatiseerde gegevensbestanden.[26] Artikel 17 bepaalt als zodanig niets omtrent de wijze waarop de gegevens verstrekt kunnen worden en laat dus eigenlijk alle opties open. Vanuit een oogpunt van kenbaarheid en rechtszekerheid wordt het niettemin wenselijk geacht deze twee specifieke verstrekkingsmogelijkheden expliciet in de wet te regelen. Met rechtstreeks geautomatiseerde toegang wordt een *on line*- en *real time* verbinding tussen de dienst en de verstrekkende persoon of instantie bedoeld, waarbij zonder menselijke tussenkomst aan de kant van de verstrekkende persoon of instantie, de desbetreffende dienst de gegevens die deze nodig heeft voor een goede taakuitvoering kan opvragen en verstrekt krijgt. Een dergelijke toegang – die in het kader van artikel 22 louter op vrijwillige basis kan worden overeengekomen – is met name van belang in de gevallen waarbij het voorzienbaar is dat in het kader van een goede taakuitvoering het wenselijk is dat de diensten structureel de beschikking hebben over (actuele) gegevens die bij een persoon of instantie beschikbaar zijn. Een voorbeeld hiervan vormt de toegang binnen het kader van de CT Infobox tot de daarvoor in aanmerking komende gegevens bij de aangesloten partners ten behoeve van de samenwerking in de CT Infobox. De verstrekking van (geautomatiseerde) gegevensbestanden op een daartoe strekkend verzoek van de diensten zal vaak aan de orde zijn, indien men op dergelijke gegevensbestanden specifieke vormen van data-analyse (zie artikel 47 van het wetsvoorstel), zoals het doorzoeken op profielen of naar patronen – al dan niet in combinatie met andere bestanden – wil toepassen. Dit soort bewerkingen dienen vanwege privacy- en beveiligingsaspecten idealiter binnen het afgeschermde ICT-domein van de diensten zelf plaats te vinden.

Een tweede aanvulling ten opzichte van de bestaande regeling betreft de in artikel 22, vijfde lid, van het wetsvoorstel neergelegde regeling, ingevolge welke gegevens die betrekking hebben op dan wel kunnen leiden tot de vaststelling van de identiteit van een natuurlijke persoon die op heimelijke wijze medewerking heeft verleend aan een verzoek tot verstrekking van gegevens 30 jaar nadat de medewerking van de desbetreffende persoon is beëindigd, worden vernietigd. Het betreft hier gegevens die betrekking hebben op *informanten* van de dienst. Een vergelijkbare regeling wordt in artikel 26, achtste lid, van het wetsvoorstel getroffen voor *agenten*. Deze regeling strekt ter uitvoering van het kabinetsstandpunt naar aanleiding van het rapport van de commissie Dessens en is – deels – gemodelleerd naar de regeling, zoals opgenomen in artikel 12, zesde lid, van de Wet politiegegevens, waarbij eveneens is voorzien in de vernietiging van gegevens van politie-informanten. Met deze regeling wordt mede op wettelijk niveau

[26] Deze aanvulling was reeds opgenomen in het ingetrokken post-Madridwetsvoorstel. Zie Kamerstukken I, 2007/08, 30 553, A, Artikel I, onder F.

concreet invulling gegeven aan een aspect van de in artikel 20 van het wetsvoorstel (huidig artikel 15 Wiv 2002) in algemene zin neergelegde plicht voor de hoofden van de dienst om zorg te dragen voor de geheimhouding van daarvoor in aanmerking komende – in casu menselijke - bronnen waaruit gegevens afkomstig zijn en de veiligheid van de personen met wier medewerking gegevens worden verzameld. De bij de uitvoering van de aan de diensten opgedragen taken ingezette menselijke bronnen – informanten en agenten – zijn niet alleen van onschatbare waarde (omdat ze bijvoorbeeld direct toegang hebben tot en het vertrouwen genieten van een target en zijn omgeving), maar lopen ook een verhoogd veiligheidsrisico. Menselijke bronnen van de diensten wordt daarom ook absolute geheimhouding toegezegd; zonder een dergelijke toezegging zou de bereidheid om samen te werken met een inlichtingen- en veiligheidsdienst ernstig in gevaar komen en daarmee een belangrijke mogelijkheid om aan informatie te komen die van essentieel belang kan zijn voor de nationale veiligheid komen te ontvallen. Absolute geheimhouding brengt naar ons oordeel met zich mee dat de gegevens die betrekking hebben op dan wel kunnen leiden tot de vaststelling van de identiteit van de bron op enig moment worden vernietigd en aldus nimmer voor derden – zoals bijvoorbeeld voor historisch onderzoek - beschikbaar komen. Het gaat er niet alleen om dat die geheimhouding wordt geëerbiedigd zolang de betrokkene in leven is, maar ook na zijn overlijden houdt deze betekenis voor zijn nagelaten betrekkingen en naaste omgeving die vaak nimmer van diens werkzaamheden voor een dienst op de hoogte zullen zijn geweest. In het wetsvoorstel is gekozen voor een langere termijn waarna de gegevens dienen te worden vernietigd, namelijk 30 jaar, dan in de Wet politiegegevens het geval is (in casu 10 jaar). Bij de keuze voor een langere termijn speelt met name een rol dat tegenover de plicht om de identiteit van betrokkene geheim te houden ook de plicht bestaat om, ingeval naar aanleiding van zijn werkzaamheden voor een dienst bij betrokkene (alsnog) klachten ontstaan, betrokkene zo goed mogelijk daarin bij te kunnen staan en hulp te kunnen bieden. Het is niet uitgesloten dat deze klachten pas na een wat langere periode openbaren. Een termijn van dertig jaar na beëindiging van diens werkzaamheden achten we, mede gelet op praktijkervaringen, voldoende ruim.

3.3.3 De bijzondere bevoegdheden tot gegevensverzameling van de diensten

3.3.3.1 Algemeen

Naast de algemene bevoegdheid om gegevens te verzamelen, beschikken de AIVD en de MIVD ook over een aantal bijzondere bevoegdheden. Het bijzondere aan deze bevoegdheden is dat zij in een aantal opzichten waar het gaat om de concrete uitoefening ervan een geheim karakter hebben. Zoals bij de totstandkoming van de

huidige wet al werd gesteld[27], is het evident dat in beginsel geheim dient te zijn en te blijven welke bijzondere bevoegdheid in welke situatie jegens welke persoon of organisatie wordt uitgeoefend. Ook de specifieke (al dan niet technische) invulling van bij de uitoefening van een bepaalde bijzondere bevoegdheid in te zetten middel dient geheim te blijven, teneinde contramaatregelen gericht op het frustreren van de inzet en de effectiviteit van het desbetreffende middel tegen te gaan. Het bijzondere karakter van deze bevoegdheden mede in het licht van de eisen die met name vanuit het EVRM daaraan gesteld dienen te worden, zie ook hierna en hoofdstuk 9 van deze toelichting, vergt dat deze van een adequaat wettelijk fundament dienen te zijn voorzien. De huidige wettelijke regeling voorziet daar reeds in, maar dient in diverse opzichten – zowel naar aanleiding van het kabinetsstandpunt inzake het rapport van de commissie Dessens als naar aanleiding van ontwikkelingen in de jurisprudentie van het EHRM – nadere aanvulling en aanscherping.

De regeling inzake bijzondere bevoegdheden in het wetsvoorstel is ten opzichte van de bestaande regeling op diverse onderdelen in meer of mindere mate gewijzigd. Dat geldt zowel waar het gaat om de gevallen waarin bijzondere bevoegdheden door de diensten mogen worden ingezet alsmede het van toepassing zijnde toestemmingsregime, als de regeling van (enkele van) de afzonderlijke bijzondere bevoegdheden. Zo is onder meer de formulering van enkele bijzondere bevoegdheden herzien zonder dat daarbij overigens de strekking ervan is gewijzigd (wetstechnische aanpassing) en zijn enkele bijzondere bevoegdheden als gevolg van technologische en andersoortige ontwikkelingen aangepast. Op deze en andere aanpassingen van het stelsel van bijzondere bevoegdheden zal in het onderstaande nog afzonderlijk worden ingegaan.

Evenals in de huidige wet het geval is, is bij de uitwerking van (onder meer) de regeling inzake de verwerking van gegevens acht geslagen op de eisen die daaraan dienen te worden gesteld zowel vanuit grondrechtelijk (artikel 10, 12 en 13 Grondwet) als mensenrechtelijk (met name artikel 8 EVRM) oogpunt. In hoofdstuk 9 van deze toelichting zal afzonderlijk bij de grondrechtelijke en mensenrechtelijke aspecten van hetgeen in dit wetsvoorstel wordt geregeld worden stilgestaan. Op deze plaats is het aangewezen om ter zake reeds het volgende op te merken. Met name in de jurisprudentie van het EHRM met betrekking tot artikel 8 EVRM is waar het gaat om (vormen van) "*secret measures of surveillance*" (waartoe de bijzondere bevoegdheden moeten worden gerekend) een daarop toegespitst normenkader ontwikkeld. Dit normenkader (naar de toenmalige stand van zaken) is ook bij de totstandbrenging van de huidige wet als leidend beginsel gehanteerd bij de inrichting van het wettelijk stelsel

[27] Kamerstukken II 1997/98, 25 877, nr. 3, blz. 24.

inzake de bijzondere bevoegdheden. In de afgelopen jaren is dit kader door het EHRM, zie met name ook de zaak Weber and Saravia tegen Duitsland, verder aangescherpt en is door het EHRM een aantal minimum waarborgen geformuleerd waar het gaat om de zwaarste inbreuken op het door artikel 8 EVRM gegarandeerde recht op privacy.[28] Het betreft hier overigens waarborgen die niet uitsluitend de (uitoefening van de) bijzondere bevoegdheid raken, maar ook zien op andere aspecten verbonden aan de (verdere) verwerking van de met de bijzondere bevoegdheden verzamelde gegevens; bijvoorbeeld een aanduiding van de kring van personen omtrent wie door de diensten gegevens mogen worden verzameld in relatie tot de uitoefening van de bijzondere bevoegdheid (zie artikel 23 jo. artikel 18 van het wetsvoorstel) alsmede de (verdere) verstrekking van de verzamelde gegevens en de voorzorgen die daarbij in acht genomen moeten worden (zie paragraaf 3.4 waarin specifieke regels zijn gesteld inzake de verstrekking van gegevens en de eisen waaraan voldaan moet worden bij de verstrekking van persoonsgegevens aan derden). De door het EHRM geformuleerde minimum waarborgen zijn onder meer bij de uitwerking van de nieuwe regeling inzake de bijzondere bevoegdheden geïmplementeerd.

In het onderstaande zal thans op de verschillende onderdelen van de nieuwe regeling inzake bijzondere bevoegdheden worden ingegaan.

3.3.3.2 Het toepassingsgebied van de bijzondere bevoegdheden

In artikel 23 van het wetsvoorstel is bepaald in welke gevallen door de diensten de in paragraf 3.2.2 opgenomen bijzondere bevoegdheden mogen worden uitgeoefend. Daarmee is allereerst aangesloten bij de huidige regeling, zoals opgenomen in artikel 18 Wiv 2002 (zie artikel 23, eerste lid). Het gaat daarbij om de inzet van bijzondere bevoegdheden *in het kader van een goede taakuitvoering* van de diensten. Net zoals nu het geval is, mogen de bijzondere bevoegdheden niet bij alle – in artikel 8, tweede lid, en

[28] Weber and Saravia tegen Duitsland, par. 95; in de uitwerking toegespitst op interceptie van telecommunicatie, maar uiteraard in brede zin van toepassing op andere (qua zwaarte vergelijkbare) "secret measures of surveillance". Het betreft hier de volgende minimum waarborgen die in wetgeving (*statute law*) moeten zijn uitgewerkt om misbruik van (de interceptie)bevoegdheid te voorkomen:

a. the nature of the offences which may give rise to an interception order;

b. a definition of the categories of people liable to have their telephones tapped;

c. a limit on the duration of telephone tapping;

d. the procedure to be followed for examining, using and storing the data obtained;

e. the precautions to be taken when communicating the data to other parties; and

f. the circumstances in which recordings must be erased or the tapes destroyed.

10, tweede lid van het wetsvoorstel geformuleerde – taken worden ingezet, maar is dat beperkt tot die taken waarbij dat – mede gelet op de aard van de desbetreffende taak - noodzakelijk is. Dat betekent dat de bijzondere bevoegdheden door de diensten slechts mogen worden uitgeoefend voor zover dat noodzakelijk is voor de goede uitvoering van de taken, bedoeld in artikel 8, tweede lid, onder a en d, en de taken, bedoeld in artikel 10, tweede lid, onder a, c en e, van het wetsvoorstel. Dit correspondeert met de bestaande regeling in artikel 18 Wiv 2002. Dat betekent dus dat de bijzondere bevoegdheden door de diensten niet kunnen worden ingezet bij de uitvoering van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken (artikel 8, tweede lid, onder b, en artikel 10, tweede lid, onder b). Bij de uitvoering van die taak kan worden volstaan met de algemene bevoegdheid tot het verzamelen van gegevens als bedoeld in artikel 22 van het wetsvoorstel. De voor deze taak benodigde gegevens kunnen worden verkregen door het voeren van gespreken met de (kandidaat) vertrouwensfunctionaris, door hem opgegeven referenten en informanten; voorts door raadpleging van diverse – interen en externe – gegevensbestanden. Ook bij de beveiligingsbevorderende taak van de diensten, zoals neergelegd in de artikelen 8, tweede lid, onder c, en 10, tweede lid, onder d, is de uitoefening van bijzondere bevoegdheden niet noodzakelijk en daarom ook niet mogelijk. Bij deze taak wordt immers in overleg en met medewerking van desbetreffende overheidsinstanties en bedrijven bezien wat voor soort beveiligingsmaatregelen in relatie tot de te beschermen belangen in het kader van de nationale veiligheid wenselijk worden geacht. De inzet van bijzondere bevoegdheden is hier niet aangewezen. Dat geldt evenzeer voor de taak die beide diensten vervullen in het kader van het stelsel van bewaking en beveiliging. In artikel 9 onderscheidenlijk artikel 11 van het wetsvoorstel is voor de AIVD onderscheidenlijk MIVD bepaald welke gegevens bij het uitbrengen van risico- en dreigingsanalyses door de AIVD en dreiginganalyses door de MIVD mogen worden betrokken; de inzet van bijzondere bevoegdheden is daar niet bij voorzien. Tot slot is in dit wetsvoorstel voorzien in aanvulling van de taakstelling van beide diensten met de taak tot – kort gezegd – het verrichten van naslagen; in paragraaf 2.2 van deze toelichting is daar uitvoerig bij stilgestaan. Het betreft hier geen onderzoek van de dienst, maar een specifieke vorm van het doen van mededeling omtrent door de diensten verwerkte gegevens. Ook hier is de inzet van bijzondere bevoegdheden niet aan de orde.

Ten opzichte van de bestaande regeling in artikel 18 Wiv 2002, is in de voorgestelde regeling voorzien van een (beperkte) uitbreiding van de uitoefening van bijzondere bevoegdheden door de diensten in enkele specifieke gevallen. Het gaat hierbij niet om de inzet in het kader van een goede taakuitvoering, maar *ter ondersteuning daarvan*. Deze aanpassing strekt ter uitvoering van het kabinetsstandpunt naar aanleiding van een

aanbeveling ter zake in het rapport van de commissie Dessens.[29] De commissie signaleert dat in de praktijk bij de diensten er soms behoefte bestaat om bijzondere bevoegdheden ook in te kunnen zetten ter ondersteuning van een goede taakuitvoering. Zij acht het wenselijk om dit mogelijk te maken in twee limitatief en zo specifiek mogelijk te omschrijven gevallen. Op de eerste plaats voor die situaties waarin de veiligheid van medewerkers van de diensten – of van andere personen die werkzaamheden voor de diensten verrichten – in het geding is. Voorts zou de mogelijkheid geopend moeten worden voor onderzoek dat nodig is om de betrouwbaarheid vast te stellen van personen met wier medewerking gegevens worden verzameld, bijvoorbeeld een agent van de dienst. In artikel 23, tweede lid, wordt voor deze twee specifieke gevallen de uitoefening van bijzondere bevoegdheden mogelijk gemaakt. Zo wordt in artikel 23, tweede lid, aanhef en onder a, bepaald dat een bevoegdheid als bedoeld in paragraaf 3.2.2 – in afwijking van het bepaalde in het eerste lid – voorts kan worden uitgeoefend ter ondersteuning van een goede taakuitvoering van de diensten, voor zover dat noodzakelijk is om te beoordelen of het noodzakelijk is bijzondere veiligheidsmaatregelen te treffen voor een persoon die werkzaam is voor of ten behoeve van de dienst in verband met de vervulling door deze persoon van een aan hem op te dragen dan wel opgedragen taak. Zoals eerder in deze toelichting is uiteengezet rust op de hoofden van de diensten een bijzondere verantwoordelijkheid waar het gaat om de veiligheid van de personen met wier medewerking gegevens worden verzameld (artikel 20, onder c). Het kan daarbij zowel gaan om eigen medewerkers als om derden. Om deze verantwoordelijkheid waar te kunnen maken kan het onder omstandigheden noodzakelijk zijn om (aanvullende) gegevens te kunnen verzamelen, die niet via de algemene bevoegdheid tot gegevensverzameling of uit open bronnen is te verkrijgen. Zo kan het voor het in kaart brengen van de risico’s die de bron loopt het noodzakelijk zijn om zicht te krijgen op de omgeving of het netwerk waarin deze zich begeeft, bijvoorbeeld door hem te volgen of om verkeersgegevens op te vragen. Onder strikte voorwaarden moet het in een dergelijke situatie mogelijk zijn om bijzondere bevoegdheden in te zetten. Dat geldt evenzeer voor de in artikel 23, tweede lid, onder b, geregelde mogelijkheid, namelijk waar het gaat om het beoordelen van de betrouwbaarheid van de personen met wier medewerking gegevens worden verzameld. Dat kan bijvoorbeeld aan de orde zijn om te controleren of een agent ook niet gerund wordt door een andere dienst. De in artikel 23, tweede lid, voorziene mogelijkheden om ook ter ondersteuning van een goede taakuitvoering bijzondere bevoegdheden in te kunnen zetten, is echter wel onderworpen aan extra voorwaarden, in het bijzonder waar het gaat om het verlenen van toestemming. In artikel 24, vijfde lid, is allereerst bepaald dat de toestemming in deze gevallen uitsluitend door de minister kan worden verleend op een daartoe strekkend

[29] Zie paragraaf 3.6.3 (blz. 38) van haar rapport.

schriftelijk verzoek van het hoofd van de desbetreffende dienst; dat geldt dus voor *alle* soorten bijzondere bevoegdheden. De toestemming kan ten hoogste voor een periode van een maand worden verleend en op een daartoe strekkend verzoek worden verlengd voor ten hoogste eenzelfde periode. Voor het overige geldt uiteraard dat zowel het initiële verzoek als het verzoek om verlenging dient te voldoen aan hetgeen in artikel 24, zesde lid, is bepaald, alsmede eventueel nog aanvullend is vereist bij de desbetreffende bijzondere bevoegdheid. Vanwege het feit dat het hier gaat om een van artikel 23, eerste lid, afwijkende uitoefening van een bijzondere bevoegdheid gaat, dient de CTIVD terstond op de hoogte te worden gesteld van een verleende toestemming (artikel 24, vijfde lid, laatste volzin).

3.3.3.3 De toestemmingsverlening met betrekking tot de uitoefening van bijzondere bevoegdheden door de diensten

Artikel 24 van het wetsvoorstel geeft een regeling voor de toestemmingverlening met betrekking tot de uitoefening van de diverse in paragraaf 3.2.2 geregelde bijzondere bevoegdheden. Daarbij zijn de uitgangspunten die aan de huidige in artikel 19 Wiv 2002 opgenomen regeling ten grondslag liggen in zijn essentie gehandhaafd. De bestaande regeling is op een aantal onderdelen echter aangevuld, waarop in het onderstaande nader zal worden ingegaan.

Evenals thans het geval is, ligt de bevoegdheid om toestemming te verlenen primair in handen van de voor de dienst verantwoordelijke minister. Anders dan bij toepassing van de algemene bevoegdheid tot gegevensverzameling, gaat het hier om de toepassing van bevoegdheden die al naar gelang de aard daarvan en de omstandigheden waarin deze worden toegepast, een ingrijpend(er) karakter kunnen hebben voor diegene ten aanzien waarvan de bevoegdheden worden ingezet. Met name de gevolgen die de uitoefening van een bijzondere bevoegdheid voor de persoonlijke levenssfeer van een persoon kan hebben, vergt niet alleen dat er voorafgaand aan de toestemmingverlening een gedegen afweging plaatsvindt maar ook dat die toestemmingverlening op het daartoe geëigende niveau plaatsvindt. Dat betekent niet dat de toestemmingverlening in alle gevallen door de betrokken minister persoonlijk dient plaats te vinden. Mandaat moet derhalve in bepaalde gevallen mogelijk zijn, zij het wel nadrukkelijk wettelijk ingekaderd waarbij verzekerd wordt dat dit mandaat uitsluitend mogelijk is aan personen die in een functionele relatie tot de betrokken dienst staan. Artikel 24, eerste lid, bepaalt dan ook dat de uitoefening van een bijzondere bevoegdheid slechts is toegestaan indien– voor zover bij paragraaf 3.2.2 niet anders is bepaald – de voor de dienst verantwoordelijke minister of namens deze het hoofd van een dienst daartoe toestemming heeft gegeven. De in artikel 19, eerste lid, Wiv 2002 neergelegde regeling wordt hier onverkort

gehandhaafd. Daarbij is in het tweede lid, eveneens overeenkomstig de bestaande regeling (artikel 19, tweede lid, Wiv 2002), voorzien in de mogelijkheid van ondermandaat door het hoofd van de dienst aan hem ondergeschikte ambtenaren; ondermandaat aan niet aan hem ondergeschikte ambtenaren, zoals bijvoorbeeld de ambtenaren als bedoeld in artikel 79 en 80, die onder verantwoordelijkheid van de Minister van BZK onderscheidenlijk de Minister van Defensie (feitelijke) werkzaamheden verrichten ten behoeve van de AIVD onderscheidenlijk de MIVD, is derhalve niet mogelijk. Door de hoofden van AIVD en MIVD is van de mogelijkheid van ondermandaat gebruik gemaakt en hebben zij ter zake een mandaatbesluit vastgesteld. De hier voorziene mogelijkheid van mandaat laat uiteraard onverlet de bevoegdheid van de minister om de gemandateerde per geval of in het algemeen instructies te geven ter zake van de uitoefening van de gemandateerde bevoegdheid. Voorts houdt de minister hier uiteraard de bevoegdheid om waar hij dat aangewezen acht zelf de toestemming met betrekking tot de uitoefening van de bijzondere bevoegdheid te verlenen. Onverlet het voorgaande is het evident dat in de gevallen dat toestemming in (onder)mandaat kan worden verleend, deze gevallen toch ter besluitvorming aan de voor de dienst verantwoordelijke minister worden voorgelegd, indien aan de uitoefening van een bepaalde bijzondere bevoegdheid mogelijk een groot politiek of andersoortig risico is verbonden.

De toestemming wordt ingevolge artikel 24, derde lid, voor zover bij of krachtens de wet niet anders is bepaald, verleend voor een periode van ten hoogste drie maanden en kan telkens op een daartoe strekkende periode worden verlengd voor een eenzelfde periode.[30] Dit komt eveneens overeen met de thans bestaande regeling (artikel 19, derde lid, Wiv 2002).

Zowel in de huidige wet als in onderhavig wetsvoorstel is met betrekking tot de uitoefening van enkele bijzondere bevoegdheden bepaald dat het verlenen van toestemming is voorbehouden aan uitdrukkelijk daarbij aangewezen personen of instanties. Deze zijn derhalve nadrukkelijk van de hiervoor geschetste mogelijkheid van mandaat uitgezonderd (het betreft hier de gevallen waarop de in artikel 24, eerste lid, opgenomen clausule “voor zover bij paragraaf 3.3.2 niet anders is bepaald” betrekking heeft). Zo is in het wetsvoorstel ten aanzien van enkele bijzondere bevoegdheden[31] bepaald dat de toestemming slechts door de voor de dienst verantwoordelijke minister moet worden verleend (vgl. artikel 25, tweede lid, 27, derde lid, 28, tweede en vierde lid, 30, derde en zesde lid, 32, tweede lid, 33, tweede lid, 34, derde lid, 35, tweede en vierde

[30] Daarmee wordt invulling gegeven aan een van de door het EHRM geformuleerde eisen, namelijk dat er een tijdslimiet aan de uitoefening van de bevoegdheid dient te worden gesteld.
[31] Ondersteunende bevoegdheden daaronder begrepen.

lid, 37, tweede lid, 38, tweede lid, 39, tweede lid, 41, tweede lid). Daarnaast wordt in artikel 24, vierde lid, en in artikel 29, eerste lid, de bevoegdheid tot het verlenen van toestemming in handen gelegd van de rechtbank Den Haag. Artikel 24, vierde lid, bepaalt dat de uitoefening van een bevoegdheid als bedoeld in paragraaf 3.2.2 jegens een journalist, waarbij de uitoefening is gericht op het achterhalen van de bron van de journalist, slechts is toegestaan, indien de rechtbank daartoe, op verzoek van de betrokken minister, toestemming heeft verleend. Deze specifieke regeling vloeit voort uit een uitspraak van het EHRM van 22 november 2012 in een door de Telegraaf c.s. tegen de Staat der Nederlanden aanhangig gemaakte zaak, waarin het EHRM unaniem tot het oordeel komt dat de inzet van bijzondere bevoegdheden van de AIVD jegens journalisten van De Telegraaf een schending oplevert van artikel 8 en 13 EVRM.[32] Bij brief van 7 december 2012 heeft de Minister van BZK, mede namens de minister van Veiligheid en Justitie, de Tweede Kamer der Staten-Generaal geïnformeerd omtrent de gevolgen die aan de uitspraak worden verbonden.[33] Dat heeft ertoe geleid dat bij Koninklijke boodschap van 15 september 2014 een voorstel van wet tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met de invoering van een onafhankelijke bindende toets voorafgaand aan de inzet van bijzondere bevoegdheden jegens journalisten, welke is gericht op het achterhalen van hun bronnen, bij de Tweede Kamer der Staten-Generaal is ingediend.[34] Kortheidshalve wordt voor een nadere uiteenzetting verwezen naar de desbetreffende kamerstukken. De in dat wetsvoorstel voorziene wijziging is in artikel 24, vierde lid, van onderhavig wetsvoorstel verwerkt.[35] In artikel 29, eerste lid, wordt bepaald dat de diensten bevoegd zijn tot het openen van brieven en andere geadresseerde zendingen, zonder goedvinden van de afzender of de geadresseerde, indien de rechtbank Den Haag daartoe, op verzoek van het hoofd van de dienst, een last heeft afgegeven. Ingevolge artikel 13, eerste lid, Grondwet is het briefgeheim onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter. Overeenkomstig deze grondwetsbepaling is zowel in het huidige artikel 23, eerste lid, Wiv 2002 als in het voorgestelde artikel 29, eerste lid, de rechtbank Den Haag aangewezen als de rechter die de vereiste last dient af te geven.

In artikel 24, vijfde lid, van het wetsvoorstel is een specifieke toestemmingsregeling opgenomen waar het gaat om de uitoefening van bijzondere bevoegdheden *ter ondersteuning* van een goede taakuitvoering van de diensten in twee specifieke situaties, waarin artikel 23, tweede lid, van het wetsvoorstel thans voorziet. Bij de bespreking van

[32] EHRM, Telegraaf Media Nederland Landelijke Media B.V. en anderen t. Nederland (No. 39315/06).
[33] Kamerstukken II 2012/13, 30 977, nr. 49.
[34] Kamerstukken II 2014/15, 34 027, nrs. 1-4.
[35] Gelet op de stand van zaken van de parlementaire behandeling is afgezien van het opnemen van een samenloopbepaling in onderhavig wetsvoorstel.

dat artikelonderdeel is reeds op deze toestemmingsregeling ingegaan, zodat kortheidshalve daarnaar wordt verwezen.

In *bijlage 3* bij deze memorie van toelichting is een schematisch overzicht opgenomen van de bijzondere bevoegdheden die in het wetsvoorstel zijn voorzien, waarbij onder meer het toestemmingsniveau voor de te onderscheiden bijzondere bevoegdheden is aangegeven.

In de huidige wet is bij de regeling van enkele bijzondere bevoegdheden bepaald wat de inhoud van een verzoek om toestemming in ieder geval dient te bevatten. Bij enkele bijzondere bevoegdheden is ter zake niets bepaald. Voorts loopt hetgeen in een dergelijk verzoek moet worden opgenomen vaak uiteen, hetgeen verklaarbaar is vanwege de relatie die de inhoud van het verzoek heeft met de aard van de bevoegdheid. Het wordt wenselijk geacht om de bestaande regelingen met betrekking tot een verzoek om toestemming waar dat kan te stroomlijnen alsmede met enkele elementen aan te vullen. Artikel 24, zesde lid, van het wetsvoorstel voorziet daarin. De daarin opgenomen regeling is niet alleen van toepassing op initiële verzoeken om toestemming, maar ook op verzoeken om verlenging daarvan. Het verzoek om toestemming dient allereerst aan te geven voor welke bijzondere bevoegdheid toestemming wordt gevraagd. Vervolgens zal een omschrijving dienen te worden gegeven van het onderzoek waarvoor de bijzondere bevoegdheid dient te worden uitgeoefend. De omschrijving van het onderzoek dient zo concreet mogelijk te zijn; zo zal een omschrijving als "onderzoek naar terrorismedreiging" niet voldoen, maar moet deze nader worden ingekaderd naar bijvoorbeeld de soort dreiging en de targetgroep. Ook zal dienen te worden aangegeven welk doel met de uitoefening van de bevoegdheid wordt beoogd en waarom (de reden) de uitoefening van de bijzondere bevoegdheid noodzakelijk wordt geacht. Hier zullen ook de afwegingen met betrekking tot de eisen van proportionaliteit en subsidiariteit hun beslag dienen te krijgen. Waar het gaat om verzoeken om verlenging van een toestemming is voor de beoordeling van het verzoek van belang te weten welke resultaten tot nu toe met de uitoefening van de bijzondere bevoegdheid zijn behaald; daarbij kan volstaan met een aanduiding van die resultaten.[36] Waar in aanvulling op hetgeen is bepaald in artikel 24, zesde lid, nog nadere gegevens in een verzoek dienen te worden opgenomen, is dat bij de desbetreffende bijzondere bevoegdheid nader aangegeven.

3.3.3.4 Bijzondere bevoegdheden

[36] Dit aspect heeft onder meer in rapport nr. 35 van de CTIVD inzake de inzet van de afluisterbevoegdheid en van de bevoegdheid tot selectie van Sigint door de AIVD (10 juli 2013) aandacht gekregen; zie ook de conclusies aanbevelingen 11.11 en 11.12.

3.3.3.4.1 Algemeen

In paragraaf 3.2.2. van het wetsvoorstel (in het bijzonder de subparagrafen 3.2.2.2 tot en met 3.2.2.8) worden de bijzondere bevoegdheden die de diensten in het kader van het verzamelen van gegevens kunnen uitoefenen nader geregeld. Het betreft een limitatieve opsomming van bijzondere bevoegdheden; de inzet van (inlichtingen)middelen die niet terug te herleiden zijn tot een van deze bevoegdheden is dan ook niet geoorloofd.[37] Ten opzichte van de huidige regeling van bijzondere bevoegdheden (paragraaf 3.2.2 Wiv 2002) is de voorgestelde regeling in verschillende opzichten gewijzigd. Zo is onder meer de formulering van enkele bijzondere bevoegdheden herzien zonder dat daarbij overigens de strekking ervan is gewijzigd (wetstechnische aanpassing), zoals bijvoorbeeld de regeling inzake volgen en observeren (artikel 25) en het openen van brieven en andere geadresseerde zendingen (artikel 29). Met betrekking tot een enkele bestaande bijzondere bevoegdheid is een thans daarin besloten liggend aspect als een zelfstandige bijzondere bevoegdheid geformuleerd (regeling DNA-onderzoek gericht op vaststelling, waaronder begrepen de verificatie, van een identiteit; artikel 28). De bijzondere bevoegdheid inzake onderzoek van een geautomatiseerd werk ("hacken") is aangevuld met de (daaraan ondersteunende) bevoegdheid tot verkenning van geautomatiseerde werken alsmede enkele handelingen die in het kader van het binnendringen van geautomatiseerde werken mogen uitgevoerd (artikel 30). De meest ingrijpende herziening op het vlak van bijzondere bevoegdheden betreft echter de bestaande bevoegdheden die betrekking hebben op interceptie van telecommunicatie en het opvragen van telecommunicatiegegevens, welke thans – samengevoegd – zijn ondergebracht in de paragraaf inzake onderzoek van communicatie (paragraaf 3.2.2.7; de artikelen 31 tot en met 41). Deze herziening vloeit (grotendeels) voort uit het kabinetsstandpunt inzake het onderdeel "Inzet van bijzondere bevoegdheden in de digitale wereld" uit het advies van de commissie Dessens, dat op 21 november 2014 aan het parlement is aangeboden en op 10 februari 2015 door de Ministers van BZK en van Defensie in een Algemeen Overleg met de vaste commissies van BZK en van Defensie van de Tweede Kamer is besproken. Tot slot is ook de regeling inzake toegang tot plaatsen, welke ondersteunend is aan de uitoefening van enkele bijzondere bevoegdheden, op onderdelen aangepast om in de toepassingspraktijk gebleken leemten in de regeling te adresseren (artikel 42). In het onderstaande zullen de diverse bevoegdheden nog afzonderlijk worden toegelicht.

[37] Zie ook artikel 78, vijfde lid, van het wetsvoorstel, waar het gaat om het doen van verzoeken van ondersteuning door de AIVD en de MIVD *aan* buitenlandse collega-diensten waar het gaat om de uitoefening van bijzondere bevoegdheden (of handelingen die daarop zijn terug te herleiden).

In de huidige wet is waar het gaat om de uitoefening van diverse bijzondere bevoegdheden door de MIVD buiten plaatsen in gebruik van het Ministerie van Defensie erin voorzien dat de daarvoor vereiste toestemming wordt verleend in overeenstemming met de Minister van BZK of, voor zover de wet daarin voorziet, in voorkomend geval het hoofd van de AIVD. Het betreft hier de zogeheten deconflictieregeling. De thans bij de diverse bijzondere bevoegdheden opgenomen deconflictieregeling komt met het voorgestelde artikel 75 te vervallen. Voor de overwegingen daarvoor wordt kortheidshalve verwezen naar paragraaf 6.2 van deze toelichting.

3.3.3.4.2 Observeren en volgen

Artikel 25 van het wetsvoorstel geeft een regeling voor het observeren en volgen door de diensten. Deze regeling komt geheel overeen met de bestaande regeling in artikel 20 Wiv 2002, met dien verstande dat de daarin opgenomen deconflictieregeling in het tweede en derde lid is komen te vervallen. Op grond van artikel 25, eerste lid, zijn de diensten bevoegd tot het observeren en volgen van natuurlijke personen of zaken. De gegevens die de diensten in dat kader verzamelen mogen worden vastgelegd. Bij observatie kan onderscheid worden gemaakt tussen statische en dynamische observatie. Statische observatie vindt plaats vanuit een min of meer vast waarnemingspunt; dynamische observatie betreft het onopvallend gadeslaan en volgen van personen. Bij de uitoefening van de bevoegdheid tot observatie mogen observatie- en registratiemiddelen worden ingezet; daarbij kan worden gedacht aan een verrekijker, foto- en video-apparatuur. Echter ook anderszins kan sprake zijn van observatie. Zo is het regelmatig of continu raadplegen van hetgeen door een persoon op door hem gebruikte social media (twitter, Facebook e.d.) wordt geplaatst eveneens aan te merken als een vorm van (on line) observatie, waarvoor dus toestemming dient te zijn verkregen. Ook bij het volgen van personen of zaken kunnen hulpmiddelen worden ingezet; het gaat dan om volgmiddelen, plaatsbepalingapparatuur en registratiemiddelen.

Op de uitoefening van deze bevoegdheid is de toestemmingsregeling van artikel 24 van toepassing, hetgeen betekent dat – buiten de in artikel 24, vierde en vijfde lid geregelde gevallen - toestemming kan worden verleend door de voor de dienst verantwoordelijke minister of namens deze het hoofd van de desbetreffende dienst; ook is ondermandaat door het hoofd van de dienst mogelijk.

Indien observatie- en registratiemiddelen als bedoeld in artikel 25, eerste lid, onder a, dienen te worden ingezet in woningen, dient daarvoor door de betrokken minister afzonderlijk schriftelijk toestemming te worden verleend aan het hoofd van de dienst (artikel 25, tweede lid). Het verzoek daartoe dient ingevolge het derde lid, in aanvulling op het bepaalde in artikel 24, zesde lid, het adres van de woning te bevatten waarbinnen

het middel dient te worden toegepast alsmede een omschrijving van het soort middel. Een dergelijke bevoegdheidsuitoefening heeft een zodanig ingrijpend karakter dat daarvoor door de minister zelf toestemming dient te worden verleend. Een door de minister verleende toestemming geldt voor een periode van ten hoogste drie maanden en kan telkens op een daartoe strekkend verzoek voor eenzelfde periode worden verlengd. Voor het plaatsen van observatie- en registratiemiddelen (en andere daarmee samenhangende activiteiten) binnen een woning is het noodzakelijk om deze - vanwege het heimelijke karakter - zonder toestemming van de bewoner binnen te treden. Op grond van de Algemene wet op het binnentreden is daarvoor een machtiging vereist. In artikel 42 van het wetsvoorstel is een regeling gegeven voor de (ondersteunende) bevoegdheid van de diensten op grond waarvan zij in het kader van de daarin aangegeven gevallen toegang hebben tot elke plaats. In artikel 42, vierde lid, is bepaald dat de machtiging als bedoeld in artikel 2 van de Algemene wet op het binnentreden door de betrokken minister dan wel namens deze het hoofd van de dienst wordt afgegeven. Een dergelijke machtiging is slechts een drietal dagen geldig. Het is dan ook mogelijk dat binnen de termijn waarvoor toestemming is verleend tot uitoefening van de observatiebevoegdheid, een dergelijke machtiging meerdere keren wordt afgegeven. Zie voorts de toelichting op artikel 42 van het wetsvoorstel.

Van de toepassing van deze bevoegdheid dient ingevolge artikel 45 een verslag te worden opgesteld. Ook de in artikel 46 geregelde notificatieplicht is, ingeval zonder toestemming van de bewoner een woning is betreden, van toepassing.

3.3.3.4.3 Agenten

Artikel 26 van het wetsvoorstel geeft een regeling voor de inzet van agenten door de diensten. Agenten dienen te worden onderscheiden van informanten. Een agent is een natuurlijke persoon die doelbewust door een dienst wordt ingezet om gericht gegevens te verzamelen die voor de taakuitvoering van een dienst van belang kunnen zijn; daarnaast kan – in uitzonderingsgevallen - de agent tevens worden belast met het bevorderen of nemen van maatregelen in verband met door de dienst te behartigen belangen. Het gaat er primair om jegens een bepaalde persoon of in een bepaalde organisatie die in het kader van een onderzoek van een dienst de aandacht heeft, een zogeheten informatiepositie te verwerven en – eenmaal verworven – die ook te behouden. Een agent kan een medewerker van de dienst zijn of een derde. Een informant daarentegen is een persoon die door de positie waarin hij verkeert dan wel de hoedanigheid die hij heeft over gegevens beschikt of kan beschikken die voor een goede taakuitvoering van de dienst van belang kunnen zijn. De raadpleging van informanten vindt plaats op grond

van artikel 22 van het wetsvoorstel. Voor zowel de agent als de informant geldt dat deze te allen tijde op vrijwillige basis hun medewerking verlenen.

De figuur van de agent is thans geregeld in artikel 21, eerste lid, onder a, Wiv 2002. Artikel 21 regelt daarnaast ook de oprichting en de inzet van rechtspersonen. Om redenen, zoals uiteengezet in hoofdstuk 4 van deze memorie van toelichting, is de regeling voor de oprichting en inzet van rechtspersonen door de diensten alsmede hetgeen is bepaald inzake het door een agent bevorderen of treffen van maatregelen, in artikel 60 onderscheidenlijk 61 van het wetsvoorstel geregeld.

In artikel 26, eerste lid, wordt bepaald dat de diensten bevoegd zijn tot de inzet van natuurlijke personen al dan niet onder dekmantel van een aangenomen identiteit en hoedanigheid, die onder verantwoordelijkheid en onder instructie van een dienst zijn belast met het gericht gegevens verzamelen omtrent personen en organisaties die voor de taakuitvoering van de dienst van belang kunnen zijn. Voor de inzet van een agent is toestemming vereist. De in artikel 24 opgenomen regeling is daarbij van toepassing. Wel is in artikel 26, zevende lid, bepaald dat de toestemming kan worden verleend voor een periode van ten hoogste een jaar en telkens op een daartoe strekkend verzoek kan worden verlengd voor eenzelfde periode. Dat is een ruimere termijn dan de drie maanden als voorzien in artikel 24, derde lid, van het wetvoorstel. De termijn van drie maanden is in de praktijk namelijk veel te kort. De inzet van een agent bij een onderzoek van de dienst strekt zich over het algemeen over een veel langere periode uit; de recrutering, opbouw en inzet van een agent is een proces dat in de praktijk veel tijd vergt. Tot slot wordt opgemerkt, dat voor zover een agent (bij instructie; zie hierna) wordt belast met de uitoefening van een bijzondere bevoegdheid, ook de voor de uitoefening van die bijzondere bevoegdheid vereiste toestemming dient te zijn verkregen. De toestemming – uitsluitend - voor de inzet van een agent is aldus niet voldoende.

De instructiebevoegdheid is uitdrukkelijk vastgelegd, teneinde de verantwoordelijkheid voor de inzet van een agent ook daadwerkelijk waar te kunnen maken. De agent dient zich aan de gegeven instructie te houden. De instructie wordt in de regel mondeling door een operateur van de dienst aan de agent gegeven, maar dient ingevolge artikel 26, zesde lid, ook schriftelijk te worden vastgelegd. Dat is zowel noodzakelijk vanuit intern-beheersmatig oogpunt (sturing van operationele activiteiten), als om het optreden van de agent in voorkomende gevallen achteraf te kunnen toetsen en evalueren. Ook is dit van

belang voor het rechtmatigheidstoezicht door de CTIVD.[38] De werkzaamheden die bij de instructie aan een agent worden opgedragen, en dat geldt in het bijzonder voor zover het gaat om het kunnen (mede)plegen van strafbare feiten – waarop hieronder nog wordt ingegaan -, zal vooral bepaald worden door de mate van betrouwbaarheid van betrokkene. Deze zal door de dienst dienen te worden vastgesteld, hetgeen geen eenmalige exercitie is maar een continu proces, waarbij bijvoorbeeld wordt gekeken in hoeverre hij zich aan de instructie heeft gehouden, de informatie die geleverd wordt e.d. In bijzondere gevallen zal het zelfs noodzakelijk zijn om daartoe bijzondere bevoegdheden in te zetten. In het wetsvoorstel is daarvoor in artikel 23, tweede lid, aanhef en onder b, naar aanleiding van een daartoe strekkende aanbeveling van de commissie Dessens, expliciet de mogelijkheid geopend. Deze is overigens wel aan bijzondere toestemmingsvoorwaarden onderworpen (artikel 24, vijfde lid).

In artikel 26, derde lid, is erin voorzien dat de agent bij instructie van de dienst tevens kan worden belast met het verrichten van handelingen die tot gevolg kunnen hebben dat medewerking wordt verleend aan het plegen van een strafbaar feit, dan wel een strafbaar feit wordt gepleegd. Een dergelijke instructie mag alleen volgens de in de wet geregelde procedure aan een agent worden gegeven, indien een goede taakuitvoering van de dienst dan wel de veiligheid van de agent daartoe noodzaakt. Zoals hiervoor is aangegeven is het optreden van de agent er primair erop gericht een bepaalde informatiepositie te verwerven en vervolgens te behouden. In dat kader zal de agent vaak bepaalde activiteiten moeten verrichten om bijvoorbeeld het vertrouwen van de betreffende persoon of organisatie te winnen. Dat betekent dat hij zich zodanig zal moeten gedragen dat ten aanzien van zijn betrouwbaarheid en geloofwaardigheid geen twijfel ontstaat. Dat is ook van belang met het oog op zijn eigen veiligheid; afwijkend groepsgedrag kan er immers toe leiden dat betrokkene wordt ontmaskerd en wordt geconfronteerd met – soms levensbedreigende – represaillemaatregelen. Dat betekent dat de agent zoveel als mogelijk is, moet conformeren aan het in de betreffende organisatie geldende groepsgedrag, waarbij de situatie zich kan voordoen dat hij medewerking moet verlenen aan het plegen van strafbare feiten dan wel dat hij strafbare feiten pleegt. De agent moet daarvoor een uitdrukkelijke instructie krijgen en hij dient zich daar ook aan te houden; bij de uitvoering daarvan mag hij door zijn optreden een persoon in ieder geval niet brengen tot een ander handelen betreffende het beramen of plegen van strafbare feiten, dan waarop diens opzet reeds tevoren was gericht (artikel 26, vierde lid; het zogeheten Tallon-criterium). In artikel 26, vijfde lid, is bepaald wat in een instructie als bedoeld in het derde lid dient te worden aangegeven. Zo zal duidelijk

[38] Vgl. CTIVD-rapport nr. 8a (MIVD) en 8b (AIVD), Inzet van informanten en agenten in het buitenland, en CTIVD-rapport nr. 37, De inzet van enkele langlopende agentenoperaties door de AIVD.

dienen te worden aangegeven (a) onder welke omstandigheden deze ter uitvoering van de instructie handelingen mag verrichten die tot gevolg kunnen hebben dat medewerking wordt verleend aan het plegen van een strafbaar feit, dan wel een strafbaar feit wordt gepleegd alsmede (b) de wijze waarop aan de instructie uitvoering dient te worden gegeven, waaronder begrepen de aard van de handelingen, die door de agent daarbij zullen mogen worden verricht, voor zover deze bij het geven van de instructie zijn te voorzien. Dat betekent dat in de instructie het soort strafbare handelingen waaraan de agent medewerking mag verlenen dan wel welke hij mag plegen – voor zover die kunnen worden voorzien op het moment dat de instructie wordt gegeven – worden benoemd. In de praktijk wordt daarover door de diensten veelal het advies van de Landelijke Officier van Justitie Terrorismebestrijding ingewonnen, opdat in de instructie een adequate aanduiding van de betreffende strafbare feiten wordt gegeven. Dit betekent overigens niet dat van de zijde van het openbaar ministerie op voorhand wordt toegezegd dat de agent, mocht deze zijn overgegaan tot het (mede)plegen van strafbare feiten, van strafvervolging wordt gevrijwaard. Wel is voor de agent in dit kader van belang dat hij zich aan de instructie houdt, aangezien deze instructie kan worden aangemerkt als een bevoegd gegeven ambtelijk bevel als bedoeld in artikel 43 van het Wetboek van Strafrecht. Dat betekent dat in het geval dat tot strafvervolging zou worden overgegaan, deze door hem als een strafuitsluitingsgrond kan worden ingeroepen. Overigens zal daarover in de praktijk tussen de agent en de dienst nader overleg plaatsvinden vanwege de gevolgen daarvan voor het onderzoek dat door de dienst wordt uitgevoerd, maar ook welke gevolgen dat kan hebben voor de (veiligheid van de) persoon van de agent en voor diens informatiepositie. Denkbaar is dat vanwege zwaarder wegende belangen een beroep op de strafuitsluitingsgrond achterwege blijft. Indien de agent zich niet aan de instructie houdt, is de agent daar zelf volledig voor verantwoordelijk en aanspreekbaar. Een goede schriftelijke vastlegging van de instructie is dan ook van groot belang om met name achteraf, bij de debriefing van de agent, te kunnen controleren of hij zich aan de instructie heeft gehouden. Het spreekt voor zich dat ook van de debriefing van een agent een accurate schriftelijke verslaglegging dient plaats te vinden.

In het huidige artikel 21, zevende lid, Wiv 2002 is bepaald dat bij of krachtens algemene maatregel van bestuur nadere regels kunnen worden gesteld met betrekking tot (a) de voorwaarden waaronder en de gevallen waarin ter uitvoering van een instructie door een agent handelingen mogen worden verricht die tot gevolg kunnen hebben dat medewerking wordt verleend aan het plegen van een strafbaar feit, dan wel een strafbaar feit wordt gepleegd en (b) de wijze waarop de uitoefening van de desbetreffende bevoegdheid wordt gecontroleerd. In de reactie op de aanbeveling van de commissie Dessens om deze algemene maatregel alsnog vast te stellen, heeft het

kabinet aangegeven dit, gelet op de opvatting van het openbaar ministerie en met het oog op de bestaande (bevredigende) praktijk inzake advisering door het openbaar ministerie – zoals hierboven beschreven – alsmede de reeds bestaande waarborgen in de wet, niet wenselijk te achten. Gelet hierop kan de delegatiegrondslag komen te vervallen.

Zoals in artikel 26, eerste lid, is aangegeven kan de agent al dan niet onder dekmantel van een aangenomen identiteit (zoals bijvoorbeeld een valse naam) of hoedanigheid (bijvoorbeeld door zich voor te doen als lid van een bepaalde beroepsgroep) worden ingezet. Tevens zal daarbij vaak in een bijbehorende legende dienen te worden voorzien. Er dient immers voorkomen te worden dat op enigerlei wijze blijkt van een relatie tussen de persoon en de dienst die hem heeft ingezet. Dit kan niet alleen ten koste gaan van diens informatiepositie, maar soms nog belangrijker van zijn eigen veiligheid. Het kan dan onder omstandigheden noodzakelijk zijn om hem van een andere (verifieerbare) identiteit te kunnen voorzien, waarvoor de medewerking van diverse overheidsinstanties onontbeerlijk is. De betrokkene zal bijvoorbeeld over officiële identiteitspapieren met daarop de door hem te hanteren identiteit dienen te beschikken. Om dit te kunnen realiseren zal het veelal nodig zijn om af te kunnen wijken van de ter zake geldende wettelijke voorschriften. In artikel 26, tweede lid, is – vergelijkbaar met het huidige artikel 21, tweede lid – derhalve bepaald dat de voor de dienst verantwoordelijke minister daarvoor in aanmerking komende bestuursorganen schriftelijk kan opdragen die medewerking te verlenen die noodzakelijk is om een natuurlijke persoon als bedoeld in artikel 26, eerste lid, van een aan te nemen identiteit te voorzien. De voor een bestuursorgaan geldende wettelijke voorschriften ter zake van de van deze verlangde werkzaamheden, blijven voor zover deze in de weg staan aan het verrichten van die werkzaamheden buiten toepassing. Gekozen is voor de bevoegdheid om een medewerkingsplicht op te dragen in plaats van een bevoegdheid om medewerking te verzoeken, aangezien in de gevallen dat eenmaal is vastgesteld dat ten behoeve van de taakuitvoering van de diensten het noodzakelijk is om een agent van een aangenomen identiteit te voorzien dit niet moet af kunnen stuiten op een weigering van het bestuursorgaan wiens medewerking essentieel is voor het realiseren van die identiteit.

Tot slot is in artikel 26, achtste lid, bepaald dat gegevens die betrekking hebben op dan wel kunnen leiden tot de vaststelling van de identiteit van een agent 30 jaar nadat de inzet van de agent is beëindigd worden vernietigd. Deze regeling komt overeen met hetgeen in artikel 22, vijfde lid, is bepaald, voor natuurlijke personen die op heimelijke wijze medewerking hebben verleend aan verzoeken van de diensten tot verstrekking van gegevens. Kortheidshalve wordt naar de daarop gegeven toelichting verwezen, die hier onverkort van toepassing is.

3.3.3.4.4 Onderzoek van besloten plaatsen, van gesloten voorwerpen, aan voorwerpen en DNA-onderzoek

In artikel 22 van de huidige wet wordt de bevoegdheid voor de diensten geregeld tot het, al dan niet met een technisch hulpmiddel, (a) doorzoeken van besloten plaatsen, (b) doorzoeken van gesloten voorwerpen en (c) het verrichten van onderzoek aan voorwerpen gericht op het vaststellen van de identiteit van een persoon. Deze bevoegdheid wordt in vrijwel ongewijzigde vorm opnieuw geregeld in artikel 27 van het wetsvoorstel. In aanvulling daarop wordt echter thans voor een specifiek onderzoek aan voorwerpen, te weten het verrichten van DNA-onderzoek aan celmateriaal gericht op het vaststellen (en de verificatie) van de identiteit van een persoon, in een afzonderlijke wettelijke regeling voorzien (artikel 28 van het wetsvoorstel). Met laatstgenoemde regeling worden de door de CTIVD in haar rapport inzake de toepassing van biologische forensische onderzoeksmethoden door de AIVD (nr. 42) geconstateerde gebreken in de wetgeving ter zake geadresseerd. Van een afzonderlijke regeling voor het onderzoek naar vingerafdrukken wordt afgezien, omdat de resultaten van een dergelijk onderzoek in de praktijk niet altijd bruikbaar zijn en als gevolg daarvan de inzet van deze mogelijkheid uitermate beperkt is. De omstandigheden waarin een dergelijk onderzoek door inlichtingen- en veiligheidsdiensten dient plaats te vinden, is immers volstrekt anders dan in het kader van strafvordering. Voorts is de inbreuk op de persoonlijke levenssfeer van betrokkene bij een onderzoek naar vingerafdrukken minder ver gaand dan bij DNA-onderzoek het geval is. Hiervoor blijft dus artikel 27, eerste lid, aanhef en onder c, de wettelijke grondslag.

Artikel 27

Artikel 27, eerste lid, van het wetsvoorstel onderscheidt evenals nu een drietal bevoegdheden, die echter in voorkomende gevallen nauw met elkaar verbonden kunnen zijn. Te denken valt daarbij aan de situatie dat bij het doorzoeken van een besloten plaats in een afgesloten kast voorwerpen worden aangetroffen, waaraan onderzoek verricht kan worden om de identiteit van een persoon (bijvoorbeeld de gebruiker van die voorwerpen) vast te stellen. In een dergelijk geval zal voor alle drie de bevoegdheden toestemming moeten worden gevraagd. De bevoegdheid tot het doorzoeken van besloten plaatsen (eerste lid, onder a) ziet niet alleen op het doorzoeken van woningen, maar bijvoorbeeld ook op het doorzoeken van loodsen en bedrijfsgebouwen. Voor zover het een woning betreft[39], dient daarvoor door de voor de dienst verantwoordelijke minister schriftelijk toestemming te worden verleend aan het hoofd van de dienst. Het verzoek

[39] Onder woningen worden onder meer verstaan woonwagens, woonschepen, tenten, caravans, keten en onder omstandigheden ook een hotelkamer.

dient te worden gedaan door het hoofd van de dienst en dient in aanvulling op het bepaalde in artikel 24, zesde lid, het adres van de woning te bevatten die dient te worden doorzocht. De aldus verleende toestemming ziet uitsluitend op de uitoefening van deze bevoegdheid als zodanig. Voor het binnentreden in een woning zonder toestemming van de bewoner is daarnaast echter ingevolge artikel 2 van de Algemene wet op het binnentreden een machtiging vereist. Ingevolge artikel 42, vierde lid, zijn voor het binnentreden in de woning de betrokken minister of namens deze het hoofd van de dienst bevoegd tot het geven van een dergelijke machtiging. Onder het begrip doorzoeken wordt in dit verband niet alleen het enkel bezichtigen van de desbetreffende besloten plaats verstaan, maar ook het openmaken van aldaar aanwezige kasten e.d. Bij het doorzoeken van gesloten voorwerpen moet worden gedacht aan het openen en vervolgens feitelijk doorzoeken van bijvoorbeeld koffers, containers e.d. Indien men bij het doorzoeken een "geautomatiseerd werk" aantreft en men zich daartoe toegang wenst te verschaffen, dan is daarbij de in artikel 30 van het wetsvoorstel geregelde bijzondere bevoegdheid tot het binnendringen in een geautomatiseerd werk van toepassing. Bij het onderzoek aan voorwerpen gericht op het vaststellen van de identiteit van een persoon moet worden gedacht aan bijvoorbeeld het onderzoek naar vingerafdrukken (zie hiervoor), maar ook bijvoorbeeld het verrichten van DNA-onderzoek dat daarop is gericht. Voor dit laatste wordt echter thans in een specifieke wettelijke grondslag voorzien. Bij het vaststellen van de identiteit gaat het om persoonskenmerken die een persoon uniek – dat wil zeggen ten opzichte van andere personen – identificeren. In het eerste lid is voorts bepaald dat de uitoefening van de bevoegdheden kunnen plaatsvinden al dan niet met behulp van een technisch hulpmiddel. Bij de parlementaire behandeling van de huidige wet is daarbij gewezen op bijvoorbeeld de toepassing van röntgenapparatuur.

In artikel 27, tweede lid, is bepaald dat, indien dat noodzakelijk is voor het onderzoek van een dienst, een bij de toepassing de bevoegdheid als bedoeld in het eerste lid aangetroffen voorwerp voor een beperkte tijd door de desbetreffende dienst mag worden meegenomen, voor zover het onderzoek van het desbetreffende voorwerp ter plaatse van de doorzoeking onmogelijk is en de daarmee beoogde verzameling van gegevens niet op een andere, minder ingrijpende wijze kan worden bewerkstelligd. Daarbij moet bijvoorbeeld worden gedacht aan de situatie dat voor onderzoek van het voorwerp de inzet van gespecialiseerde technische apparatuur vereist is, die men niet ter plekke kan inzetten. Doet zich een situatie voor dat er voorwerpen moeten worden meegenomen, dan geldt vervolgens wel dat in dat geval de desbetreffende voorwerpen zo spoedig mogelijk worden teruggeplaatst, tenzij het belang van een goede taakuitvoering van de dienst zich daartegen verzet of met terugplaatsing geen redelijk belang wordt gediend.

Hoewel in het artikel geen concrete termijn voor terugplaatsing van het voorwerp is opgenomen, zal terugplaatsing ervan zo spoedig mogelijk dienen te geschieden. Voorkomen dient immers te worden dat voortijdig wordt ontdekt dat het voorwerp is weggenomen, hetgeen al naar gelang de situatie er mede toe kan leiden dat een onderzoek van de dienst wordt gefrustreerd. Er kunnen zich echter situaties voordoen waarbij terugplaatsing van het voorwerp in strijd zou zijn met een goede taakuitvoering door de dienst, bijvoorbeeld indien terugplaatsing ervan juist toe zou leiden dat men vermoed dat er een onderzoek naar hem loopt. Terugplaatsing kan voorts achterwege blijven indien er geen redelijk belang mee is gediend; het kan daarbij bijvoorbeeld gaan om een plastic bekertje, sigarettenpeuken of haren die men heeft aangetroffen en voor biologisch forensisch onderzoek heeft meegenomen.

Artikel 28

In artikel 28 wordt een specifieke regeling gegeven voor het verrichten van verrichten van DNA-onderzoek op basis van celmateriaal op voorwerpen ten behoeve van het vaststellen van de identiteit van een persoon. Zoals ook de CTIVD in het eerder genoemde toezichtsrapport heeft aangegeven, biedt het huidige artikel 22, eerste lid, aanhef en onder c, een wettelijke grondslag voor biologisch forensisch onderzoek als zodanig, waaronder DNA-onderzoek, voor zover dat gericht is op het vaststellen van de identiteit van een persoon. Uit de jurisprudentie van het EHRM[40] dient evenwel te worden afgeleid dat een aantal daarmee samenhangende aspecten van een expliciete wettelijke regeling dienen te worden voorzien. In haar toezichtsrapport nr. 42 (onderdeel 6.2) doet de CTIVD daartoe een aantal aanbevelingen. De CTIVD geeft daarbij aan dat er een specifieke wettelijke grondslag dient te zijn voor het inrichten en in stand houden van een DNA-databank en het bewaren van celmateriaal. Zo dienen er waarborgen voor opslagduur, gebruik, toegang van derden, procedures voor het behoud van de integriteit en vertrouwelijkheid van de data en de procedures voor de vernietiging te worden gesteld.[41] Met het voorgestelde artikel 28, bezien in samenhang met de andere in dit wetsvoorstel neergelegde waarborgen met betrekking tot de verwerking van gegevens door de diensten, wordt in totaliteit voorzien in deze en andere waarborgen, deels door nadere regelstelling bij algemene maatregel van bestuur. Thans zal op de diverse aspecten van de voorgestelde regeling worden ingegaan.

---

[40] EHRM 4 december 2008, nr. 30562/04 en 30566/04, *S. en Marper t. Verenigd Koninkrijk*.
[41] EHRM 4 december 2008, nr. 30562/04 en 30566/04, *S en Marper t. Verenigd Koninkrijk*, par. 99: "(The Court) reiterates that it is essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedure for its destruction, thus providing sufficient safeguards against the risk of abuse and arbitrariness."

Ingevolge artikel 28, eerste lid, van het wetsvoorstel zijn de diensten bevoegd tot het verrichten van DNA-onderzoek op basis van celmateriaal op voorwerpen ten behoeve van het vaststellen van de identiteit van een persoon. DNA-onderzoek dat op andere zaken is gericht dan vaststelling van de identiteit (bijvoorbeeld iemands gezondheidstoestand) is derhalve niet toegestaan. Om misverstanden te voorkomen en mede in reactie op hetgeen de CTIVD in haar toezichtsrapport (nr. 42) heeft gesteld, is – anders dan in strafvordering – in het eerste lid expliciet bepaald dat onder vaststellen ook de verificatie van de identiteit van een persoon moet worden verstaan.

Het DNA-onderzoek vindt plaats door vergelijking van DNA-profielen. Deze vergelijking kan plaatsvinden aan de hand van DNA-profielen die bij externe (binnen- en buitenlandse) instanties berusten, zoals aan de hand van de DNA-profielen opgenomen in de DNA-databank voor strafzaken, maar ook aan de hand van DNA-profielen die men zelf verwerkt en voor (toekomstige) vergelijking opslaat. Het vastleggen van DNA-profielen door de diensten zelf is noodzakelijk, omdat de vergelijking van de DNA-profielen die voor diensten zijn vastgesteld met DNA-profielen die bij externe instanties zijn vastgelegd, niet altijd een resultaat opleveren; niet alle targets van de dienst hebben immers een strafrechtelijk verleden en zijn in verband daarmee in de DNA-databank voor strafzaken opgenomen. Vergelijking met DNA-profielen die de diensten zelf hebben vastgelegd moet dan ook tot de mogelijkheden behoren om anderszins tot vaststelling of verificatie van de identiteit te komen. Zo heeft de AIVD recent in het kader van internationale samenwerking tegen terrorisme de beschikking gekregen over de DNA-profielen van een aantal zelfmoordterroristen, die echter geen hit opleverde in de DNA-databank voor strafzaken. Indien het toch Nederlandse targets zijn, maar geen strafrechtelijk verleden hebben, dan zitten zij immers ook niet in de DNA-databank voor strafzaken. De kans op een hit wordt dan vergroot indien de dienst zelf van uitreizende targets DNA-profielen heeft opgeslagen waarmee kan worden vergeleken. Overigens zullen bij algemene maatregel van bestuur nog nadere regels worden gesteld ter zake van de verwerking van de DNA-profielen door de diensten (zie artikel 28, zevende lid). Het kan daarbij onder meer gaan over de wijze waarop het DNA-onderzoek wordt verricht en de verslaglegging daarvan, de naar aanleiding van het DNA-onderzoek vast te leggen gegevens, de rechtstreekse toegang tot die gegevens en de vernietiging van celmateriaal. De uitoefening van deze bevoegdheid is vanwege het ingrijpende karakter ervan onderworpen aan het toestemmingsvereiste van de voor de dienst verantwoordelijke minister (tweede lid) en komt – gelet op de in artikel 43 neergelegde toetsingskader – eigenlijk pas dan in beeld, indien de identiteit van een persoon niet op een andere, minder ingrijpende wijze kan worden vastgesteld dan wel geverifieerd.

Het DNA-onderzoek wordt verricht aan celmateriaal van de desbetreffende persoon. Bij de feitelijke uitvoering van het onderzoek kunnen externe instanties worden ingeschakeld, zoals bijvoorbeeld het Nederlands Forensisch Instituut (NFI), maar ook andere instanties die daarin zijn gespecialiseerd kunnen daarvoor worden ingeschakeld. Het materiaal waaraan onderzoek wordt verricht kan materiaal zijn dat op grond van de toepassing van de bevoegdheid ex artikel 27, eerste lid, aanhef en onder c jo. het tweede lid, is verkregen, namelijk bij onderzoek van besloten plaatsen waarbij voorwerpen voor nader onderzoek mogen worden meegenomen, of dat door de betrokkene in de openbare ruimte is achtergelaten. In het verzoek om toestemming dient de herkomst van het celmateriaal te worden vermeld (artikel 28, derde lid onder b). Het celmateriaal wordt gebruikt voor het opstellen van de DNA-profiel. Indien met betrekking tot het celmateriaal DNA-onderzoek heeft plaatsgevonden, dient dit materiaal zo spoedig mogelijk doch uiterlijk binnen drie maanden na het onderzoek te worden vernietigd. Een zo kort mogelijke vernietigingstermijn is met name aangewezen, nu het bewaren van celmateriaal als drager van genetische en gezondheidsinformatie, in bijzondere mate inbreuk maakt op het recht op bescherming van de persoonlijke levenssfeer van personen die het betreft.[42] Aangezien de vernietiging van het celmateriaal op een gecontroleerde wijze dient plaats te vinden, waarbij ook de aanwezigheid van de forensisch expert van de dienst is vereist, is vernietiging niet altijd direct na het onderzoek mogelijk; om die reden is een termijn van maximaal drie maanden opgenomen. Van de vernietiging dient een verslag te worden gemaakt.

De DNA-profielen die aldus beschikbaar komen, zijn voor een specifiek doel opgesteld en mogen uitsluitend voor het onderzoek ten behoeve waarvan toestemming is verleend worden verwerkt. Gebruik van DNA-profielen in het kader van andere onderzoeken van de dienst of bijvoorbeeld ter verstrekking aan een andere instantie, vergt altijd een afzonderlijke en op die verdere verwerking toegespitste toestemming van de voor de desbetreffende dienst verantwoordelijke minister (artikel 28, vierde lid). Verstrekking aan een buitenlandse collega-dienst kan bijvoorbeeld aan de orde zijn in het kader van de internationale samenwerking in de strijd tegen het terrorisme, waarbij bijvoorbeeld via vergelijking van DNA-profielen die zijn verworven van omgekomen Jihad-strijders, de identiteit kan worden vastgesteld of geverifieerd. De voor een dienst opgestelde DNA-profielen mogen voor een periode van ten hoogste vijf jaren worden bewaard en dienen daarna te worden vernietigd. Onder omstandigheden kan het echter voor een goede taakuitvoering van de dienst noodzakelijk zijn (daarvoor in aanmerking komende) DNA-profielen voor een langere periode te bewaren; daarvoor dient de minister op een daartoe strekkende verzoek toestemming te geven (artikel 28, zesde lid).

[42] Zie ook EHRM 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, par. 120 en 121.

Tot slot wordt opgemerkt dat een aantal aspecten van verbonden aan de verwerking van gegevens inzake DNA-profielen en celmateriaal bij algemene maatregel van bestuur zullen worden geregeld. Artikel 28, zevende lid, biedt daarvoor de grondslag. Zo moeten in ieder geval regels gesteld voor het verwerken van DNA-profielen, waaronder begrepen de inrichting, het beheer en de toegang tot deze gegevens, en celmateriaal. De algemene maatregel van bestuur is voorts onderworpen aan een zogeheten voorhangprocedure bij beide kamers der Staten-Generaal.

3.3.3.4.5 Openen van brieven en andere geadresseerde zendingen

In artikel 29 van het wetsvoorstel is de thans in artikel 23 Wiv 2002 opgenomen bevoegdheid tot het openen van brieven en andere geadresseerde zendingen vrijwel ongewijzigd overgenomen; zoals ook bij andere bijzondere bevoegdheden, vervalt hier de zogeheten deconflictieregeling (het huidige artikel 23, derde lid, Wiv 2002).

In afwijking van de hoofdregel dat voor de uitoefening van bijzondere bevoegdheden – kortgezegd - de toestemming vereist is van de voor de dienst verantwoordelijke minister of namens deze het hoofd van de desbetreffende dienst (zie artikel 24, eerste lid, van het wetsvoorstel), is voor de uitoefening van deze bevoegdheid een last van de rechter vereist (artikel 29, eerste lid). Deze eis vloeit voort uit artikel 13, eerste lid, van de Grondwet. Evenals nu is bepaald dat de diensten bevoegd zijn tot het openen van brieven en andere geadresseerde zendingen (zoals postpakketten, drukwerk e.d.), zonder goedvinden van de afzender of de geadresseerde, indien de rechtbank te Den Haag daartoe aan het hoofd van de dienst een last heeft afgegeven. Met "andere geadresseerde zendingen" wordt aansluiting gezocht bij hetgeen daaromtrent in het kader van de Postwet wordt verstaan; het gaat dan onder meer om drukwerken, pakjes en postpakketten.

Er is voor gekozen om voor de afgifte van de vereiste last slechts één rechtbank, namelijk die te Den Haag, bevoegd te verklaren. De reden daarvoor is daarin gelegen, dat de kring van kennisdragers omtrent door de diensten verrichte onderzoeken en daarbij ingezette bevoegdheden tot een minimum beperkt dient te blijven. Daarnaast speelt ook het meer praktische belang, dat de beide diensten hun vestiging in de regio Den Haag hebben en het vereiste dat een last op zeer korte termijn afgegeven moet kunnen worden, een belangrijke rol.

Het verzoek om afgifte van een rechterlijke last wordt gedaan door het hoofd van de desbetreffende dienst. Het verzoek dient te voldoen aan de vereisten van artikel 24, zesde lid, van het wetsvoorstel; voorts dient in aanvulling daarop de naam en het adres van de persoon of instelling, van wie dan wel waarvan brieven of andere geadresseerde

zendingen aan deze gericht dan wel van deze afkomstig zijn, dienen te worden geopend, te worden vermeld (artikel 29, derde lid). Aan de hand van de informatie vermeld in het verzoek dient de rechter in staat te zijn om te toetsen of de afgifte van de verlangde last noodzakelijk is voor een goede taakuitvoering van de aan de diensten opgedragen taak (artikel 29, vierde lid). Het is voor een goede beoordeling door de rechter van belang dat hij zo goed mogelijk wordt geïnformeerd. Indien de rechter in een enkel geval kennis wil nemen van de aan een verzoek ten grondslag liggende operationele gegevens, kunnen deze aan hem ter inzage worden gegeven.

Een last als bedoeld in artikel 29, eerste lid, van het wetsvoorstel kan worden afgegeven ingeval de brief of de andere geadresseerde zending reeds in het bezit is van de dienst, bijvoorbeeld als resultante van een doorzoeking als bedoeld in artikel 27, eerste lid, van het wetsvoorstel, dan wel ingeval deze aan een instelling van post dan wel vervoer is toevertrouwd (artikel 29, vijfde lid). In de eerste situatie wordt de last per brief of geadresseerde zending die reeds in handen is van de dienst afgegeven. Indien het gaat om het openen van brieven of andere geadresseerde zendingen die aan een in de last vermelde instelling van post dan wel vervoer zijn of worden toevertrouwd, kan de last worden afgegeven voor een daarin te bepalen periode van ten hoogste drie maanden. Deze last ziet dus zowel op brieven en andere geadresseerde zendingen die reeds aan de betreffende – in de last benoemde - instelling zijn toevertrouwd dan wel in de periode waarop de last betrekking heeft worden toevertrouwd. Opneming van de instelling van post of vervoer in de last strekt ertoe om helderheid te verschaffen op wie de in artikel 29, zesde lid, neergelegde medewerkingsplicht van toepassing is; dat kunnen ook meerdere instellingen van post of vervoer betreffen. In de huidige regeling (artikel 23, vierde lid, Wiv 2002) ontbreekt waar het gaat om de inhoud van het verzoek om een last nog de verplichting om daarin aan te duiden welke instelling het betreft. In artikel 29, derde lid, van het wetsvoorstel, wordt hierin alsnog voorzien. Met een instelling van post of vervoer wordt hier onder meer gedoeld op instellingen als TNT-post, Sandd, DHL e.d.; echter ook zogeheten afhaalpunten, waarmee deze instellingen overeenkomsten hebben gesloten voor het aanbieden of afhalen van post en andere geadresseerde zendingen vallen onder dit bereik.[43]

De feitelijke uitlevering van de brieven en andere geadresseerde zendingen door de in de last aangewezen instelling van post of vervoer, vindt plaats tegen ontvangstbewijs aan een door het hoofd van de dienst aangewezen ambtenaar van de dienst, die ten opzichte van de desbetreffende instelling gehouden is zich te legitimeren (artikel 29, zevende lid). Met deze regeling wordt beoogd zeker te stellen, dat de uitlevering van de

[43] De lijst van geregistreerde postvervoerders is te raadplegen via de website van de Autoriteit Consument & Markt; www.acm.nl.

desbetreffende stukken geschiedt aan een instantie die gerechtigd is om deze stukken in ontvangst te nemen. Vanaf het ontvangst van de desbetreffende stukken draagt de dienst daarvoor de verantwoordelijkheid. De aan de dienst uitgeleverde brieven en andere geadresseerde zendingen kunnen vervolgens worden geopend en de inhoud daarvan worden onderzocht. Zodra het onderzoek is afgesloten dienen de stukken onverwijld aan de instelling van post of vervoer te worden geretourneerd, die deze vervolgens bij de geadresseerde kan bezorgen (artikel 29, achtste lid).

De uitoefening van de in artikel 29, eerste lid, geregelde bevoegdheid is in artikel 46 van het wetsvoorstel onderworpen aan de notificatieplicht. Dat betekent dat – tenzij er uitstel- of afstelgronden als bedoeld in dat artikel aan de orde zijn – aan de persoon jegens wie de bevoegdheid is uitgeoefend, een verslag daarvan dient te worden uitgebracht.

Tot slot wordt opgemerkt dat de instellingen van post en vervoer, aangezien zij betrokken zijn bij de uitvoering van de wet, zijn onderworpen aan de in artikel 124 neergelegde geheimhoudingsplicht.

3.3.3.4.6 Verkennen van en binnendringen in geautomatiseerde werken

De bevoegdheid van de diensten tot het kunnen binnendringen in een geautomatiseerd werk en het kunnen overnemen van gegevens, zoals deze thans in artikel 24 van de Wiv 2002 is geregeld, is in de afgelopen jaren van zeer groot belang gebleken. In tal van gevallen is het kunnen *hacken* van systemen noodzakelijk geweest voor het tijdig realiseren van een adequate informatiepositie ten behoeve van door de diensten uit te voeren onderzoeken. Op hoofdlijnen voorziet de huidige regeling op een goede wijze in de (gewenste) praktijk. Op enkele punten is vanuit operationele optiek aanscherping benodigd. Zo is het voor het succesvol inzetten van de bijzondere bevoegdheid tot het binnendringen van een geautomatiseerd werk nodig gebleken een normbeeld van de digitale omgeving van het onderzoekssubject te verkrijgen en de bij deze in gebruik zijnde geautomatiseerde werken te kunnen verkennen op eventuele zwakheden. Hierbij is nog geen sprake van het binnendringen van een geautomatiseerd werk als bedoeld in het huidige artikel 24 Wiv 2002. Daarnaast is uit operationele optiek gebleken dat het in voorkomende gevallen niet mogelijk is het bij een onderzoekssubject in gebruik zijnde geautomatiseerde werk direct binnen te dringen, maar dat deze mogelijkheid wel kan worden gecreëerd door gebruikmaking van een onderkende zwakheid in een ander geautomatiseerd werk. Tevens is het vanuit operationeel belang wenselijk technische voorzieningen in een geautomatiseerd werk aan te kunnen brengen ter ondersteuning van de uitvoering van andere bijzondere bevoegdheden. De huidige wet voorziet hier niet

expliciet in. Dit wetsvoorstel legt deze bevoegdheden daarom nadrukkelijk vast, waarop in het onderstaande thans zal worden ingegaan.

Met het thans voorgestelde artikel 30 wordt beoogd een regeling te geven die, onder gelijktijdige versterking van de waarborgen verbonden aan de inzet van de bevoegdheid en aan het gebruik van de in dat kader verkregen gegevens, de diensten in de gelegenheid stellen op een efficiënte en zorgvuldige wijze de voor een goede taakuitvoering benodigde gegevens te verkrijgen. Zowel bij de huidige als de voorgestelde bevoegdheden wordt met begrip geautomatiseerd werk aangesloten bij hetgeen daaronder in artikel 80 sexies van het Wetboek van Strafrecht wordt verstaan.

In aanvulling op de bestaande bevoegdheid tot het binnendringen in geautomatiseerde werken, wordt aan de diensten de bevoegdheid toegekend tot het verkennen van de technische kenmerken van geautomatiseerde werken die op een communicatienetwerk zijn aangesloten (artikel 30, eerste lid, onder a). Deze bijzondere bevoegdheid heeft ten opzichte van de bevoegdheid tot het binnendringen in een geautomatiseerd werk (artikel 30, eerste lid, onder b) een ondersteunend karakter. Onder het verkennen wordt verstaan het door de AIVD en MIVD inzetten van technische toepassingen, zoals IP- en poortscansoftware en registratiemiddelen, waarmee inzicht kan worden verkregen in de kenmerken van op communicatienetwerken aangesloten geautomatiseerde werken. Hierbij is van belang dat het digitale domein geen statische omgeving betreft, maar voortdurend aan verandering onderhevig is. Hierbij kan gedacht worden aan het gebruik van dynamische IP-adressen op het internet, waarbij een geautomatiseerd werk gebruik maakt van steeds veranderende IP-adressen. Dergelijke dynamische IP-adressen worden vaak voor inbelverbindingen en mobiele internetverbindingen gebruikt. Inherent aan de aard van geautomatiseerde werken is, dat zij kenbaar maken wat hun functie (mailserver, router etc.) is en welke poorten voor de diverse vormen van gegevensuitwisseling beschikbaar zijn. De kenmerken die door de diensten worden vastgelegd zullen daarom veelal bestaan uit vrijelijk te onderkennen gegevens over technische eigenschappen, zoals het IP-adres, de beschikbaarheid van poorten en de functie van het werk, zoals mailserver of router. Op grond van deze kenmerken zijn de diensten in staat te duiden of een geautomatiseerd werk relevantie voor de nationale veiligheid heeft, dat wil zeggen bijvoorbeeld onderdeel uit maakt van een militaire *surface-to-air* radarinstallatie, een industrieel controle systeem in een doelland betreft of bestaat uit een desktop pc van een relevante buitenlandse actor. Teneinde veranderingen tijdig te kunnen onderkennen en steeds over een *up to date* beeld van op basis van concrete onderzoeksopdrachten van de diensten relevante delen van het digitale landschap te kunnen beschikken, zullen de AIVD en MIVD de verkennende bevoegdheid semi-continu inzetten. De door de AIVD en MIVD door middel van de inzet van de

verkennende bevoegdheid verworven kenmerken, stellen de diensten aldus in staat in het belang van de nationale veiligheid gericht, efficiënt en zorgvuldig in relevante geautomatiseerde werken binnen te dringen.

In artikel 30, eerste lid, onder b, van het wetsvoorstel is de bevoegdheid van de diensten geregeld tot het al dan niet met gebruikmaking van een technische ingreep, valse signalen, valse sleutels, valse hoedanigheid of door tussenkomst van het geautomatiseerd werk van een derde, binnendringen in een geautomatiseerd werk. De bevoegdheid tot het binnendringen van een geautomatiseerd werk is gericht van aard, dat wil zeggen dat de inzet van de bijzondere bevoegdheid zich doorgaans zal richten op een geautomatiseerd werk dat bij een onderzoeksubject *(target)* van de AIVD of MIVD in gebruik is. Hierbij zetten de diensten diverse technische capaciteiten in, waarbij bijvoorbeeld onderkende zwakheden in de door het onderzoeksubject gebruikte beveiliging door de diensten zullen worden benut. 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. Het wordt in het belang van de bescherming van de nationale veiligheid noodzakelijk geacht de diensten ook in dergelijke situaties in staat te stellen om via geautomatiseerde werken van zogenoemde *non-targets* binnen te dringen in geautomatiseerde werken die bij targets in gebruik zijn. Hiertoe wordt in artikel 30, eerste lid, onder b, van het wetsvoorstel geëxpliciteerd dat het binnendringen in een geautomatiseerd werk ook kan plaatsvinden met gebruikmaking van het geautomatiseerd werk van een derde.

In artikel 30, tweede lid, is aangegeven dat tot de bevoegdheid tot het binnendringen in een geautomatiseerd werk tevens de bevoegdheid behoort tot (a) het doorbreken van enige beveiliging, (b) het aanbrengen van technische voorzieningen teneinde versleuteling van gegevens opgeslagen of verwerkt in het geautomatiseerde werk ongedaan te maken, (c) het aanbrengen van technische voorzieningen in verband met de toepassing van de bevoegdheid als bedoeld in de artikelen 25, eerste lid en 32, eerste lid, alsmede (d) het overnemen van de gegevens opgeslagen of verwerkt in het geautomatiseerde werk. De onder a, b en d genoemde bevoegdheden komen ook reeds voor in de huidige regeling (artikel 24 Wiv 2002). Nieuw is de onder c geformuleerde bevoegdheid om in het kader van het binnendringen in een geautomatiseerd werk bepaalde technische voorzieningen aan te brengen die ondersteunend zijn bij de uitoefening van de hier bedoelde bevoegdheden. Geautomatiseerde werken, zoals laptops en desktop computers, zijn tegenwoordig vrijwel allemaal uitgerust met camera’s en microfoons. Deze kunnen door het aanbrengen van technische voorzieningen, zoals

bepaalde software, op afstand worden geactiveerd en op die wijze ingezet worden als een technisch hulpmiddel bij de uitoefening van bijvoorbeeld de bevoegdheid tot observatie (artikel 25, eerste lid) of het opnemen van de conversatie in een bepaalde ruimte (artikel 32, eerste lid). Voor deze vormen van bevoegdheidsuitoefening is niet alleen de toestemming vereist die ingevolge de genoemde artikelen vereist is voor de toepassing van de desbetreffende bevoegdheden als zodanig, maar is derhalve ook tevens toestemming vereist voor de toepassing van de bevoegdheid ex artikel 30, eerste lid, onder b. Voor zover de inzet van de hier bedoelde ondersteunende bevoegdheden reeds is voorzien op het moment dat toestemming wordt gevraagd voor de uitoefening van de bevoegdheid als bedoeld in de artikelen 25, eerste lid, en 32, eerste lid, kan de desbetreffende toestemming gelijktijdig worden aangevraagd.

In artikel 30, derde lid, van het wetsvoorstel wordt bepaald dat de in het eerste lid bedoelde bevoegdheid slechts mag worden uitgeoefend, indien door de voor de desbetreffende dienst verantwoordelijke minister daarvoor op een daartoe strekkend verzoek schriftelijk toestemming is verleend aan het hoofd van de dienst. Hiermee wordt op formeelwettelijk niveau gecodificeerd, hetgeen door de Ministers van BZK en van Defensie in reactie op rapport nr. 38 van de CTIVD is aangekondigd en thans ook de praktijk is; daarmee is met betrekking tot de inzet van de “hackbevoegdheid” over de volle breedte het toestemmingsniveau naar ministerieel niveau getild en aldus voorzien in een extra waarborg. Het verzoek om toestemming dient te worden gedaan door het hoofd van de dienst en dient allereerst te voldoen aan de eisen, bedoeld in artikel 24, zesde lid; in aanvulling daarop dient daarbij – voor zover van toepassing – tevens te worden aangegeven welke bevoegdheden als bedoeld in het tweede lid, bij de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk, worden toegepast.

Artikel 30, negende lid, van het wetsvoorstel geeft ten opzichte van de bestaande wettelijke regeling een nieuw voorziening, welke de diensten ertoe dwingt om de gegevens die door toepassing van de bevoegdheid tot het binnendringen in een geautomatiseerd werk zijn verkregen zo spoedig mogelijk te onderzoeken op hun relevantie voor het onderzoek waarvoor ze zijn verworven. Gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel niet op hun relevantie voor het onderzoek zijn onderzocht, dienen binnen een periode van ten hoogste twaalf maanden nadat ze zijn verworven te worden vernietigd.

In artikel 30, vijfde tot en met achtste lid, wordt ten slotte voorzien in de bevoegdheid van de diensten om zich te wenden tot degene van wie redelijkerwijs vermoed wordt dat hij kennis draagt van de wijze van versleuteling van de gegevens opgeslagen of verwerkt in het geautomatiseerde werk als bedoeld in het eerste lid met het verzoek alle

noodzakelijke medewerking te verlenen tot het ontsleutelen van de gegevens door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken. Met de formulering is aansluiting gezocht bij artikel 126m, zesde lid, van het Wetboek van Strafvordering. Op betrokkene rust ingevolge het achtste lid een medewerkingsplicht; het niet meewerken aan een verzoek is in artikel 132 van het wetsvoorstel strafbaar gesteld. Ook hier geldt dat de bevoegdheid slechts mag worden uitgeoefend, indien door de minister op een daartoe strekkend verzoek toestemming is verleend aan het hoofd van de dienst. Het verzoek dient te voldoen aan de eisen ex artikel 24, zesde lid, alsmede de in het zevende lid, onder a en b, genoemde gegevens te bevatten.

3.3.3.4.7 Onderzoek van communicatie

3.3.3.4.7.1 Algemeen

In paragraaf 3.2.2.7 van het wetsvoorstel (de artikelen 31 tot en met 41) zijn de bepalingen samengebracht die betrekking hebben op de bijzondere bevoegdheden (inclusief de daaraan ondersteunende bevoegdheden) met betrekking tot het onderzoek van communicatie. Ten opzichte van de huidige regeling (de artikelen 25 tot en met 29 Wiv 2002) is de voorgestelde regeling in verschillende opzichten gewijzigd en uitgebreid. Een deel van de wijzigingen die thans zijn opgenomen waren reeds voorzien in het ingetrokken post-Madridwetsvoorstel.[44] Dat betreft in het bijzonder de uitbreiding van de reikwijdte van de bevoegdheden inzake telecommunicatie alsmede de daarmee corresponderende medewerkingsverplichtingen tot de aanbieders van communicatiediensten. Een ander deel is nieuw en vloeit voort uit het kabinetsstandpunt met betrekking tot het onderdeel "Inzet bijzondere bevoegdheden in de digitale wereld"[45] uit het rapport van de commissie Dessens, dat op 21 november 2014 aan de Tweede Kamer is aangeboden. Dat betreft in het bijzonder de in de artikelen 33 tot en met 37 opgenomen regeling, welke in de plaats komt van de huidige regeling in artikel 26 (*search* gericht op interceptie) en 27 (ongerichte interceptie van niet-kabelgebonden telecommunicatie en selectie). Deze bevoegdheden worden thans technologieonafhankelijk geformuleerd, waarmee de bestaande beperking tot niet-kabelgebonden telecommunicatie komt te vervallen en derhalve ook kabelgebonden telecommunicatie voor interceptie als hier bedoeld (interceptie in "bulk") in aanmerking komt. Een en ander is daarbij overeenkomstig het hiervoor genoemde kabinetstandpunt voorzien van extra waarborgen, die een zorgvuldige afweging van alle in het geding zijnde belangen – nationale veiligheid en het recht op bescherming van de persoonlijke levenssfeer – mogelijk maakt. Daarnaast is in aanvulling op de bestaande bevoegdheden

[44] Kamerstukken I 2007/08, 30 553, A, Artikel I, onderdeel L, M en N.
[45] Hoofdstuk 5 van het rapport van de commissie Dessens.

tot het opvragen van verkeersgegevens en gebruikersgegevens (ook wel: abonneegegevens) voorzien in een nieuwe bevoegdheid inzake het opvragen van telecommunicatie die bij een aanbieder van een communicatiedienst ten behoeve van een gebruiker van diens dienst is opgeslagen. Tot slot is in artikel 41 de medewerkingsverplichting tot ontsleuteling van communicatie opgenomen.

3.3.3.4.7.2 Aanbieders van communicatiediensten

Ingevolge de artikelen 28 en 29 van de Wiv 2002 kan de bijzondere bevoegdheid tot het doen van een verzoek tot het verstrekken van gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker onderscheidenlijk tot het verstrekken van gegevens ter zake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van telecommunicatie worden uitgeoefend jegens de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten als bedoeld in de Telecommunicatiewet (Tw). In artikel 1.1, onder ee en ff, van de Tw is gedefinieerd wat onder openbare telecommunicatienetwerken onderscheidenlijk openbare telecommunicatiediensten moet worden volstaan.[46] In de Telecommunicatiewet is vervolgens geregeld dat deze aanbieders verplicht zijn om aan een dergelijk verzoek uitvoering te geven. Niet voldoen aan een dergelijk verzoek is als economische delict strafbaar gesteld. Ook waar het gaat om de uitvoering van een op grond van artikel 25, tweede lid, verleende toestemming tot het opnemen en afluisteren van telecommunicatie geldt dat een verplichting tot medewerking aan de uitvoering daarvan uitsluitend bestaat voor de hiervoor genoemde aanbieders; artikel 13.2 Telecommunicatiewet biedt daarvoor de grondslag. Voorts worden bij of krachtens hoofdstuk 13 Tw met de hiervoor genoemde verplichtingen verband houdende zaken geregeld, zoals de beveiliging van gegevens en de vergoeding van kosten. In de praktijk komen in de sfeer van elektronische communicatie allerlei diensten beschikbaar, waarvan op voorhand niet duidelijk is of deze onder het begrip openbare telecommunicatiedienst kunnen worden geschaard dan wel waarvan op voorhand wel duidelijk is dat deze daar niet onder vallen, maar waarvan het wel noodzakelijk wordt geacht dat de gegevens die in dat kader worden verwerkt voor een goede taakuitvoering van de diensten beschikbaar moeten kunnen komen. Het gaat daarbij om diensten als webhosting, opslag in de cloud en dergelijke. Indien dergelijke diensten niet als een openbare telecommunicatiedienst kunnen worden aangemerkt,

[46] Een openbaar telecommunicatienetwerk is een elektronisch communicatienetwerk dat geheel of gedeeltelijk wordt gebruikt om openbare telecommunicatiediensten aan te bieden, voor zover het netwerk niet gebruikt wordt voor het verspreiden van programma's. Een openbare telecommunicatiedienst is een voor het publiek beschikbare dienst die geheel of gedeeltelijk bestaat in het overbrengen van signalen via een elektronisch communicatienetwerk, voor zover deze dienst niet bestaat uit het overbrengen van programma's.

betekent dat de in dat kader verwerkte gegevens door de diensten uitsluitend op basis van vrijwillige medewerking kunnen worden verkregen. Waar het gaat om de medewerking van aanbieders van *besloten* telecommunicatienetwerken en -diensten biedt artikel 13.7 Tw weliswaar de mogelijkheid om de bepalingen van hoofdstuk 13 Tw (met uitzondering van artikel 13.6 Tw) van overeenkomstige toepassing te verklaren, echter artikel 13.7 Tw is tot op heden nog niet in werking getreden.

In het ingetrokken post-Madridwetsvoorstel was reeds voorzien in een aanpassing van de artikel 28 en 29 Wiv 2002, waarmee de hiervoor onderkende problematiek voor een deel zou kunnen worden ondervangen, door introductie van het begrip "aanbieder van een communicatiedienst". Dit begrip is ontleend aan het Cybercrimeverdrag[47] en inmiddels in artikel 126la van het Wetboek van Strafvordering (in een deels aangepaste vorm) geïmplementeerd. Onder een "aanbieder van een communicatiedienst" wordt verstaan: de natuurlijke of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid beidt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst. Deze definitie omvat niet alleen de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten als hiervoor aangegeven, maar ook die van de besloten netwerken en diensten. Voorts vallen ook aanbieders van webhostingdiensten en beheerders van websites onder deze definitie. Ook het begrip "gebruiker van een dienst" is nader gedefinieerd: de natuurlijke of rechtspersoon die met de aanbieder die met de aanbieder van een communicatiedienst een overeenkomst is aangegaan met betrekking tot het gebruik van die dienst of die feitelijk gebruik maakt van een zodanige dienst.

In artikel 31 van het wetsvoorstel worden beide begrippen ook voor de toepassing van de (relevante) bijzondere bevoegdheden inzake onderzoek van communicatie geïntroduceerd. Daarmee wordt ook bewerkstelligd dat de begripsmatige aansluiting (bij vergelijkbare bevoegdheden op het vlak van "telecommunicatie") in de sfeer van de wetgeving inzake de inlichtingen- en veiligheidsdiensten alsmede het Wetboek van Strafvordering op dit punt wordt behouden.

3.3.3.4.7.3 Onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers

Artikel 32 van het wetsvoorstel regelt de bevoegdheid tot het met een technisch hulpmiddel gericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd

[47] Trb. 2002, 18. De Nederlandse vertaling is gepubliceerd in Trb. 2004, 290.

werk, ongeacht waar een en ander plaatsvindt. Het gaat daarbij om onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers ("gericht"). Deze bevoegdheid omvat niet alleen het aftappen en opnemen van telecommunicatie, maar bijvoorbeeld ook de toepassing van (richt)microfoons. Tot de bevoegdheid wordt voorts gerekend de bevoegdheid om versleuteling van gesprekken, telecommunicatie of gegevensoverdracht ongedaan te maken. Een en ander is thans geregeld in artikel 25, eerste lid, Wiv 2002.

Evenals thans het geval is, is de uitoefening van deze bevoegdheid uitsluitend toegestaan, indien door de voor de dienst verantwoordelijke minister daarvoor op een daartoe strekkend verzoek toestemming is verleend aan het hoofd van de dienst. Ingevolge artikel 24, vierde lid, van het wetsvoorstel is echter waar het gaat om de uitoefening van de bevoegdheid jegens een journalist, welke gericht is op het achterhalen van diens bron, de toestemming vereist van de rechtbank te Den Haag.[48]

Het verzoek om toestemming dient te voldoen aan hetgeen in artikel 24, zesde lid, is bepaald en dient voorts de in artikel 32, derde lid, bedoelde gegevens te bevatten. Dat betreft (a) voor zover van toepassing, het nummer, bedoeld in artikel 1.1, onder bb, van de Telecommunicatiewet[49] en (b) gegevens betreffende de identiteit van de persoon dan wel de organisatie ten aanzien van wie onderscheidenlijk waarvan de uitoefening van de desbetreffende bevoegdheid wordt verlangd. Het gegeven onder a is met name van belang bij de interceptie van telecommunicatie. In de praktijk kan het echter voorkomen dat bij een verzoek om toestemming het voor de interceptie benodigde nummer nog niet bekend is. Dat hoeft echter niet aan de toestemmingverlening in de weg te staan, zij het dat ingevolge artikel 32, vierde lid, de bevoegdheid dan slechts mag worden uitgeoefend, indien het desbetreffende nummer bekend is (toestemmingverlening onder opschortende voorwaarde). Het hier bedoelde nummer kan door de dienst op verschillende manieren worden achterhaald, waarbij als hoofdregel de medewerking van de aanbieder van de desbetreffende communicatiedienst wordt ingeroepen. Waar het gaat om mobiele telefonie is dat niet altijd mogelijk, bijvoorbeeld in geval van pre-paid telefonie. In dat geval zijn over het algemeen bij de aanbieder geen gegevens van de abonnee bekend en kan het voor het aftappen benodigde nummer niet worden geleverd. De diensten zullen dan op een andere wijze het nummer dienen te verkrijgen en wel door de inzet van een technisch hulpmiddel, bijvoorbeeld – waar het gaat om mobiele telefonie – zogeheten

[48] Dat geldt overigens voor alle bijzondere bevoegdheden die jegens een journalist worden uitgeoefend, voor zover daarmee wordt beoogd diens bron te achterhalen.
[49] Onder nummer wordt verstaan: cijfers, letters of andere symbolen, al dan niet in combinatie, die bestemd zijn voor toegang tot of identificatie van gebruikers, netwerkexploitanten, diensten, netwerkaansluitpunten of andere netwerkelementen.

actieve scanapparatuur (zoals een IMSI-catcher[50]). In de praktijk kan echter niet altijd worden volstaan met het scannen van de ether om het vereiste nummer te achterhalen, maar zal het soms ook noodzakelijk zijn om gedurende een korte periode kennis te nemen van de inhoud van de via een dergelijk technisch hulpmiddel ontvangen gegevens teneinde het juiste nummer vast te stellen. Dit zal zich met name voordoen bij het gebruik van mobiele (data)diensten, zoals WiFi, waarbij tevens sprake is van een grotere groep gebruikers. Ten opzichte van de huidige regeling is in verband hiermee in artikel 32, vierde lid, voorzien in de mogelijkheid dat door de diensten daarbij van de ontvangen gegevens kennis mag worden genomen voor zover en zolang dat noodzakelijk is voor het vaststellen van het juiste nummer. De bevoegdheid is nadrukkelijk beperkt tot dat doel en gebruik van de inhoud voor andere doeleinden is niet toegestaan. Voorts is bepaald dat gegevens die geen betrekking hebben op het hier bedoelde nummer terstond dienen te worden vernietigd. Daarmee wordt tevens de met de uitoefening van deze ondersteunende bevoegdheid gepaard gaande inbreuk op de persoonlijke levenssfeer van de personen tot een minimum beperkt. Met deze ondersteunende bevoegdheid kan op een adequate wijze de mogelijkheid tot uitoefening van de hoofdbevoegdheid, in casu het aftappen en opnemen van telecommunicatie, worden gegarandeerd. Met het tijdelijk kennisnemen van de bij de inzet van een technisch hulpmiddel ontvangen gegevens kan inbreuk worden gemaakt op het telefoongeheim van de betrokkene. Deze inbreuk is, gelet op het doel waartoe dat plaatsvindt, namelijk het realiseren van een reeds door de minister geaccordeerde inzet van de bevoegdheid tot gerichte interceptie van de telecommunicatie van een persoon in het belang van de nationale veiligheid, alleszins gerechtvaardigd. De ingevolge artikel 13 Grondwet vereiste toestemming voor deze activiteit ligt besloten in de toestemming die de betrokken minister voor de interceptie van de telecommunicatie als zodanig reeds heeft verleend.[51]

Niet alleen het nummer kan onder omstandigheden nog niet bekend zijn, dat kan evenzeer zich voordoen waar het gaat om de identiteit van de persoon of organisatie, waartegen door de dienst de bevoegdheid wordt ingezet. Ingeval van een telefoontap wordt dan gesproken over een zogeheten NN-tap. Ingevolge artikel 32, vijfde lid, wordt ingeval bij het verzoek om toestemming de gegevens, bedoeld in het derde lid, onder b, nog niet bekend zijn, de toestemming slechts verleend onder de voorwaarde de desbetreffende gegevens zo spoedig mogelijk aan te vullen.

[50] Een IMSI-catcher doet zich voor als een basisstation voor mobiele telefonie die het verkeer tussen een mobiele telefoon en het basisstation van de telecomaanbieder afvangt en daarbij de beschikking krijgt over bijvoorbeeld de IMSI-nummers die door de mobiele telefoons binnen het bereik van de IMSI-catcher worden gebruikt.

[51] In het ingetrokken post-Madridwetsvoorstel was ook reeds in een vergelijkbare regeling voorzien; zie Kamerstukken II 2007/08, 30 553, A, Artikel I, onder L.

In de praktijk komt het voor dat onderzoekssubjecten van de diensten regelmatig van nummer (en mobiel toestel) wisselen of van meerdere nummers (en mobiele toestellen) gebruik maken, vaak met het doel om interceptie van hun telecommunicatie door de bevoegde instanties te bemoeilijken. Het veiligheidsbewustzijn bij dergelijke onderzoekssubjecten kan zelfs zover gaan dat men per gesprek slechts eenmaal van een bepaald nummer en toestel gebruik maakt. Om te voorkomen dat in dergelijke gevallen telkens opnieuw toestemming dient te worden gevraagd om op het nieuwe nummer te mogen tappen, is de zogeheten bijschrijfmogelijkheid ontwikkeld. In dat geval wordt door de minister niet alleen toestemming verleend voor toepassing van de interceptiebevoegdheid op het reeds bekende nummer, maar ook op andere nadien bekend geworden nummers van het desbetreffende onderzoekssubject. Aangezien de uitoefening van de hier bedoelde bevoegdheid en de verleende toestemming ertoe strekken om de telecommunicatie van een specifieke persoon of organisatie te intercepteren, bestaat daartegen geen bezwaar; het nummer is daarbij een – zij het cruciaal – hulpmiddel. Aan deze praktijk wordt thans in artikel 32, zesde lid, een expliciete wettelijke grondslag gegeven. Daarbij zij wel aangetekend dat het daarbij dient te gaan om nummers die toebehoren aan de desbetreffende persoon of organisatie. Indien het onderzoekssubject gebruik maakt van het nummer dat aan een andere persoon of organisatie toebehoort, zal hiervoor wel toestemming dienen te worden verkregen. Immers in dat geval zal ook de telecommunicatie van die andere persoon worden geïntercepteerd en daarbij dus een inbreuk gemaakt op diens recht op bescherming van de persoonlijke levenssfeer. Dit vergt een afzonderlijke afweging.[52]

In artikel 13.2 Tw is bepaald dat de aanbieders van openbare telecommunicatienetwerken onderscheidenlijk openbare telecommunicatiediensten verplicht zijn medewerking te verlenen aan de uitvoering van een toestemming tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld onderscheidenlijk van door hen verzorgde telecommunicatie. Naast deze aanbieders komen echter ook andere aanbieders van communicatiediensten in aanmerking om medewerking te verlenen aan de uitvoering van een dergelijke toestemming. In artikel 32, zevende lid, wordt de medewerkingsplicht uitgebreid tot de aanbieders van een communicatiedienst op wie niet reeds een medewerkingsverplichting ex artikel 13.2 Tw rust. Dat betekent bijvoorbeeld dat een aanbieder van een besloten telecommunicatienetwerk of –dienst verplicht is om medewerking te verlenen. In artikel 13.6 Tw wordt een regeling gegeven voor de kosten en vergoedingen voor de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten om te

[52] Zie ook CTIVD-rapport nr. 19, inzake de toepassing door de AIVD van artikel 25 WIV 2002 (aftappen) en artikel 27 WIV 2002 (selectie van ongericht ontvangen niet-kabelgebonden telecommunicatie), blz. 24-25.

kunnen voldoen aan de verplichtingen op het terrein van bevoegd aftappen. Kort gezegd komt die regeling erop neer dat deze aanbieders de investerings-, exploitatie- en onderhoudskosten die zij moeten maken om (technisch) aftapbaar te zijn, zelf dienen te dragen (artikel 13.6, eerste lid, Tw); voor vergoeding komen louter de gemaakte administratiekosten en personeelskosten in aanmerking die rechtstreeks voortvloeien uit het uitvoeren van een taplast (artikel 13.6, tweede lid, Tw). In artikel 32, achtste lid, van het wetsvoorstel wordt deze regeling van overeenkomstige toepassing verklaard op de andere aanbieders van communicatiediensten. Er bestaat geen aanleiding om voor deze aanbieders een (deels) afwijkende regeling te treffen.

In artikel 25, achtste lid, Wiv 2002 is thans – voor zover hier relevant – bepaald, dat voor het gericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie (etherverkeer) dat zijn oorsprong of bestemming in andere landen heeft en tevens militair berichtenverkeer betreft, geen toestemming is vereist als bedoeld in artikel 19 en 25, tweede lid, Wiv 2002. Indertijd is ter zake opgemerkt dat dit een continue activiteit betreft, waarbij het stellen van het toestemmingsvereiste geen toegevoegde waarde heeft. Belangrijker is dat militair verkeer naar zijn aard niet vergelijkbaar is met het telecommunicatieverkeer tussen gewone burgers, waarbij de persoonlijke levenssfeer van betrokkenen in het geding is. Een met artikel 25, achtste lid, Wiv 2002 vergelijkbare maar in enkele opzichten gewijzigde regeling, is opgenomen in artikel 32, negende lid, van het wetsvoorstel. Allereerst is de beperking tot niet-kabelgebonden telecommunicatie komen te vervallen; er is voor gekozen om de bepaling technologieonafhankelijk te formuleren. Ook voor het militaire domein heeft het onderscheid tussen niet-kabelgebonden en kabelgebonden communicatie door de ontwikkelingen in het digitale domein immers aan betekenis verloren. Dit brengt met zich mee dat ook voor het gericht ontvangen en opnemen van kabelgebonden telecommunicatie als hier bedoeld geen toestemming vereist is. Ten tweede wordt in plaats van militair berichtenverkeer thans in algemene zin gesproken van militair verkeer. De term berichtenverkeer is verouderd en techniekafhankelijk. Het deel ‘berichten’ suggereert een gestructureerde stroom van inhoudelijke boodschappen en antwoorden. Het doet te zeer denken aan morse-uitzendingen uit de 20^{e} eeuw, terwijl thans van belang is de communicatie tussen (piloten van) jachtvliegtuigen met grondsystemen en de operatieleiding, de radar en het dataverkeer van luchtafweer, vliegtuigen en schepen, de *chatter* van ongedisciplineerde strijdkrachten e.d. Aangezien het niet is uit te sluiten dat bij het ontvangen en opnemen van militair verkeer in voorkomend geval ook niet-militair verkeer meekomt, waarbij sprake kan zijn van een inbreuk op het recht op persoonlijke levenssfeer van degene die voor zijn privé-communicatie gebruik maakt van een regulier voor militaire doeleinden

bestemd communicatiekanaal, is ten slotte bepaald, dat dit niet militaire verkeer terstond dient te worden vernietigd.

Artikel 32, tiende lid, van het wetsvoorstel geeft ten opzichte van de bestaande wettelijke regeling een nieuw voorziening, welke de diensten ertoe dwingt om de gegevens die door toepassing van de bevoegdheid als bedoeld in het eerste lid zijn verkregen zo spoedig mogelijk te onderzoeken op hun relevantie voor het onderzoek waarvoor ze zijn verworven. Gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel niet op hun relevantie voor het onderzoek zijn onderzocht, dienen binnen een periode van ten hoogste twaalf maanden nadat ze zijn verworven te worden vernietigd.

3.3.3.4.7.4 Onderzoek van communicatie in andere gevallen

Algemeen

In paragraaf 3.2.2.7.3 van het wetsvoorstel wordt een geheel nieuwe regeling gegeven voor het onderzoek van communicatie in andere gevallen dan waarbij sprake is van een op een specifieke persoon, organisatie of nummer gerichte uitoefening van de interceptiebevoegdheid. Deze regeling treedt in plaats van de regeling inzake het verkennen van niet-kabelgebonden telecommunicatie (artikel 26 Wiv 2002) en de ongerichte interceptie van niet-kabelgebonden telecommunicatie en de selectie van de aldus ontvangen en opgenomen telecommunicatie (artikel 27 Wiv 2002). Daarnaast worden in paragraaf 3.2.2.7.3 van het wetsvoorstel een aantal ondersteunende bevoegdheden geformuleerd, die van toepassing zijn bij de uitoefening van de in artikel 33 geformuleerde bevoegdheid tot het verwerven van telecommunicatie in andere gevallen. Het betreft hier de bevoegdheid om zowel die informatie alsmede die medewerking te verzoeken van aanbieders van communicatiediensten, die voor de toepassing van artikel 33 noodzakelijk zijn. Met deze nieuwe regeling wordt uitvoering gegeven aan het door het kabinet ingenomen standpunt inzake het onderdeel "Bijzondere bevoegdheden in de digitale wereld" uit het rapport van de commissie Dessens. Daarin wordt het standpunt van de commissie Dessens onderschreven dat de techniekafhankelijke interceptiebepalingen van de Wiv 2002 op basis van het onderscheid tussen de ether en de kabel niet meer te rijmen valt met de voortschrijdende technologische ontwikkelingen op het gebied van dataverkeer en communicatie.

In paragraaf 2 van de kabinetsreactie worden deze ontwikkelingen en de betekenis daarvan voor de inlichtingen- en veiligheidsdiensten nader geduid. Zoals daar is gesteld, is in de afgelopen jaren – mede door de enorme ontwikkeling van het internet – het communicatieverkeer dat via de kabelgebonden infrastructuur verloopt explosief

gestegen. Naast een explosieve groei van de hoeveelheid gegevens die in de wereld wordt geproduceerd (en elke twee tot drie jaar verdubbelt) moet worden vastgesteld dat inmiddels ongeveer 90% van alle telecommunicatie via kabelnetwerken verloopt. In de huidige wet is met deze ontwikkeling geen rekening gehouden. De daarin opgenomen regeling voor ongerichte interceptie van telecommunicatie codificeerde de toenmalige praktijk bij de diensten, met name de toenmalige Militaire Inlichtingendienst (MID), waarbij interceptie van radio- en satellietverkeer centraal stond. Anders dan bij de bijzondere bevoegdheid tot gerichte interceptie (artikel 25 Wiv 2002), die wel technologieonafhankelijk werd geformuleerd, is dat bij de regeling voor ongerichte interceptie achterwege gebleven.

Voor de (inter)nationale veiligheidsbelangen van Nederland en het optreden van de krijgsmacht is een stevige Nederlandse inlichtingenpositie van fundamenteel belang, of het nu gaat om het voorkomen van terrorisme, tegengaan van spionage, beschermen tegen digitale aanvallen, inzicht in bedreigingen voor de internationale rechtsorde, het doorgronden van intenties van een aantal landen, zicht op de capaciteitsontwikkeling van risicolanden of de proliferatie van massavernietigingswapens. De diensten moeten bovendien zicht hebben op de dreigingen waaraan de samenleving en de staat in het digitale domein kunnen worden blootgesteld, om zich daar vervolgens effectief tegen te kunnen wapenen en anderen in staat te stellen maatregelen te treffen. De technische dreigingen en mogelijkheden manifesteren zich zowel op het kabelgebonden als ook op het niet-kabelgebonden deel van het digitale domein. De (potentiële) impact van cyberdreigingen is door uiteenlopende incidenten in de afgelopen jaren steeds duidelijker geworden. Het gaat daarbij niet alleen om dreigingen die onze cyberinfrastructuur kunnen verstoren, maar ook om dreigingen ten aanzien van de integriteit, beschikbaarheid en vertrouwelijkheid van de informatie die we allen digitaal vastleggen, gebruiken en uitwisselen. Om zicht te houden op deze dreigingen zijn de diensten afhankelijk van een adequate toegang tot telecommunicatie.

De diensten moeten daarom beschikken over voldoende inlichtingenmiddelen en -capaciteiten om informatie op het juiste moment in het digitale domein te verwerven, te analyseren en daarover tijdig te rapporteren. Bijzondere bevoegdheden die het mogelijk maken om – onder strikte voorwaarden – in bulk te intercepteren in het kabelgebonden domein zijn daarbij onmisbaar.

Het nieuwe normatieve kader voor interceptie en de daarbij op te nemen waarborgen kent de volgende elementen. Allereerst zal het nieuwe, technologieonafhankelijke stelsel voor de interceptie van telecommunicatie ("bulk") op hoofdlijnen uit een drietal fasen bestaan: (a) doelgerichte verwerving van telecommunicatie, (b) voorbewerking van de

geïntercepteerde telecommunicatie en (c) (verdere) verwerking van de telecommunicatie. Deze drie te onderscheiden fasen komen grotendeels terug in onderscheidenlijk de artikelen 33 (verwerving), 34 (voorbewerking) en 35 (selectie en metadata-analyse) van het wetsvoorstel. Daarbij dient gerealiseerd te worden dat met name de activiteiten in fase 2 van betekenis zijn voor het interceptieproces in brede zin, in die zin dat de resultaten van de activiteiten in die fase niet louter op zichzelf staan, maar mede facilitair zijn aan de toepassing van de bijzondere bevoegdheid tot verwerving als bedoeld in artikel 33 als de bijzondere bevoegdheid tot selectie als bedoeld in artikel 35. In het wetsvoorstel zijn de desbetreffende bevoegdheden voorzien van de waarborgen, zoals in eerder genoemd kabinetsstandpunt reeds zijn aangekondigd. Het betreft hier waarborgen, die zowel het gebruik van de interceptiebevoegdheid (verwerving) als de verdere verwerking van de geïntercepteerde gegevens voor daarbij te onderscheiden doeleinden afhankelijk maakt van (a) een voorafgaande en in tijd begrensde ministeriële toestemming, (b) doelgerichte inzet, (c) bewaar- en vernietigingstermijnen met betrekking tot de desbetreffende gegevens en (d) een (gecombineerd) stelsel van functie- en taakscheiding c.q. compartimentering waar het gaat om de toegang tot de gegevens in de verschillende fasen en buiten het interceptieproces. Bij de bespreking van de desbetreffende artikelen zal op de uitwerking van deze waarborgen in dat kader nader worden ingegaan.

Voor de uitoefening van de bevoegdheid tot interceptie van kabelgebonden telecommunicatie zal in de praktijk de medewerking vereist zijn van de desbetreffende aanbieder van de communicatiedienst (in casu de netwerkaanbieder). Deze medewerking is zowel vereist bij het verkrijgen van informatie van relevante aanbieders met het oog op het in kaart brengen van het zogeheten communicatielandschap (in brede zin) als de concrete formulering van de inhoud van het verzoek om medewerking (de last); zie artikel 36 van het wetsvoorstel. Voorts is medewerking vereist bij de uitvoering van de last, zij het dat daartoe niet eerder wordt overgegaan dan nadat ter zake met de desbetreffende aanbieder overleg is gevoerd; zie artikel 37 van het wetsvoorstel.

In het kabinetsstandpunt is voorts aangegeven dat het gebruik van de geïntercepteerde telecommunicatie zowel kan zien op de desbetreffende metadata (“verkeersgegevens”) als op de inhoud van de telecommunicatie. In het licht van de constatering, dat het van oudsher gemaakte onderscheid tussen metadata enerzijds en de inhoud van de telecommunicatie anderzijds bij de beantwoording van de vraag naar de mate van inbreuk op de in geding zijnde grondrechten onder invloed van de steeds grote wordende schaal waarop gegevens voor verwerking in aanmerking komen en de steeds verdergaande mogelijkheden tot verwerking van die gegevens aan relativering toe is, voorziet het wetsvoorstel ook dienaangaande in aanvullende waarborgen. Zo is in artikel

47 van het wetsvoorstel een regeling opgenomen voor geautomatiseerde data-analyse. Indien een dergelijke analyse wordt toegepast op de metadata die in het kader van de bevoegdheid ex artikel 33 is geïntercepteerd en het doel daarvan is het identificeren van personen of organisaties, dan is ook deze verwerking onderworpen aan ministeriële toestemming (artikel 35, vierde lid).

Tot slot wordt hier opgemerkt dat de ministeriële toestemmingen die in de hierna beschreven fasen voor de uitoefening van de desbetreffende bevoegdheden vereist zijn, zijn onderworpen aan het zogeheten heroverwegingsstelsel. Dat betekent dat de CTIVD deze kan onderwerpen aan een onmiddellijke rechtmatigheidstoets, waarbij alle relevante aspecten aan de orde kunnen komen (doelbinding, voldoende duidelijke afbakening onderzoek, toets aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit e.d.). Indien de CTIVD vervolgens tot het oordeel komt dat een door de minister verleende toestemming ten onrechte is verleend en dit aan de minister mededeelt, is de minister wettelijk gehouden deze opnieuw te overwegen (artikel 102 van het wetsvoorstel). Indien de minister van opvatting is dat de toestemming gehandhaafd dient te blijven, dan zal hij de CTIVD en de CIVD hiervan onverwijld op de hoogte dienen te brengen. De CIVD kan vervolgens desgewenst de minister ter verantwoording roepen. Op deze wijze is voorzien in een effectieve waarborg tegen een onrechtmatig gebruik van de hier bedoelde bevoegdheden voorafgaand en tijdens de door de diensten te verrichten onderzoeken in het belang van de nationale veiligheid.

In het onderstaande zal thans op de verschillende fasen en de daarvoor relevante artikelen worden ingegaan.

Fase 1: de doelgerichte verwerving van telecommunicatie (artikel 33)

In artikel 33, eerste lid, van het wetsvoorstel, is de bevoegdheid van de diensten neergelegd tot het met een technisch hulpmiddel aftappen, ontvangen, opnemen en afluisteren van elke vorm van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk ongeacht waar een en ander plaatsvindt in andere gevallen dan bedoeld in artikel 32, indien wordt voldaan aan hetgeen bij of krachtens dit artikel wordt gesteld. Tot deze bevoegdheid wordt tevens de bevoegdheid gerekend tot het ongedaan maken van de versleuteling van de telecommunicatie of gegevensoverdracht alsmede de technische analyse van de gegevens voor zover deze gericht is op de optimalisatie van de uitoefening van de hiervoor bedoelde interceptiebevoegdheid.

Deze bevoegdheid komt in de plaats van de bestaande bevoegdheden tot het met een technisch hulpmiddel ontvangen en opnemen van niet-kabelgebonden telecommunicatie

als bedoeld in de artikelen 26, eerste lid, en 27, eerste lid, Wiv 2002. De nieuwe bevoegdheid wijkt in een aantal opzichten af van de bestaande bevoegdheden.

Allereerst is het technologieonafhankelijk geformuleerd; de beperking tot uitsluitend niet-kabelgebonden telecommunicatie is komen te vervallen. Dat betekent dat de diensten niet alleen bevoegd zijn om – onder voorwaarden (zie hierna) – etherverkeer te onderscheppen, maar ook kabelgebonden telecommunicatie. Dit laatste is ook van belang in verband met het onderzoek door de diensten in het kader van cybersecurity.

Ten tweede is ervoor gekozen om de bevoegdheid zowel betrekking te doen hebben op telecommunicatie als op gegevensoverdracht door middel van een geautomatiseerd werk. Zoals ook indertijd bij het wetsvoorstel computercriminaliteit II tot uitdrukking is gebracht, zal bij overdracht van gegevens door middel van telecommunicatie dit veelal tevens plaatsvinden door middel van een geautomatiseerd werk, maar begripsmatig overlappen deze begrippen elkaar niet helemaal.[53] Om ter zake geen enkele onduidelijkheid te doen bestaan worden beide begrippen naast elkaar gebruikt, waardoor buiten kijf staat dat telecommunicatie die niet door middel van een geautomatiseerd werk (waarbij de definitie van artikel 80 sexies Wetboek van Strafrecht wordt gehanteerd) plaatsvindt, ook binnen het bevoegdheidsbereik van de diensten valt. Dit is met name aan de orde indien niet wordt voldaan aan de drie cumulatieve criteria voor geautomatiseerd werk: opslaan, verwerken en overdragen. Hiervan kan bijvoorbeeld sprake zijn bij een eenvoudig telefoontoestel of bij optische verbindingstechnologieën, waarbij geen sprake is van opslag.

De in de bevoegdheid tot interceptie tevens besloten liggende bevoegdheid tot het ongedaan maken van de versleuteling van de telecommunicatie of gegevensoverdracht, is – waar het gaat om telecommunicatie – een reeds bestaande bevoegdheid (zie de artikelen 26, eerste lid, derde volzin, en 27, eerste lid, tweede volzin). Door middel van crypto- en signaalonderzoek en ontcijfertechnieken zal getracht worden om versleutelde data leesbaar te maken. Anders dan thans het geval is, wordt in artikel 41 van het wetsvoorstel, voorzien in een geclausuleerde medewerkingsplicht voor een ieder van wie redelijkerwijs vermoed wordt dat hij kennis draagt van de wijze van versleuteling. Bij de bespreking van dat artikel zal op de voorwaarden waaronder deze medewerking mag worden ingeroepen, nader worden ingegaan.

Een andere in de interceptiebevoegdheid besloten liggende bevoegdheid betreft de technische analyse van de gegevens voor zover deze gericht is op de optimalisatie van de uitoefening van de interceptiebevoegdheid. Deze bevoegdheid is in de huidige regeling

[53] Zie Kamerstukken II 2004/05, 26 671, nr. 7, blz. 35.

niet als zodanig benoemd, maar vindt wel plaats. Het betreft hier een technische behandeling van gegevens die uitsluitend gericht is op het detecteren, ordenen en labelen van gegevens, welke tezamen met de bevoegdheid tot het ontsleutelen van gegevens, bij kan dragen aan het op een juiste wijze ontsluiten van gegevens en het uitfilteren daarvan. Met name het toepassen van filters bij de interceptie leidt ertoe dat de bulk aan gegevens die wordt geïntercepteerd, wordt gereduceerd tot die gegevens die voor verder onderzoek relevant kunnen zijn. Bij filters die gebuikt worden om datastromen te reduceren moet bijvoorbeeld worden gedacht aan het uitfilteren van televisie-uitzendingen. Naast een dergelijk negatief filter kan ook sprake zijn van samengestelde filters, bijvoorbeeld: verwijder alle spraakverkeer afkomstig van een satelliet, behalve vanuit een bepaald gebied.

De uitoefening van de nieuwe bevoegdheid is in tegenstelling tot de huidige bevoegdheid ex artikel 26 en 27 Wiv 2002 onderworpen aan een ministerieel toestemmingsvereiste. Dat betekent dat anders dan nu, ook voor de interceptie van etherverkeer in bulk toestemming van de minister is vereist; ook indien dit zonder medewerking van een aanbieder van een communicatiedienst plaatsvindt, bijvoorbeeld door gebruikmaking van het eigen satellietgrondstation van de diensten in Burum. Hiermee is een eerste extra waarborg ingebouwd waar het gaat om de uitoefening van de in het eerste lid bedoelde bevoegdheid. Ingevolge artikel 33, tweede lid, mag de bevoegdheid slechts worden uitgeoefend, indien door de voor de desbetreffende dienst verantwoordelijke minister op een daartoe strekkend verzoek toestemming is verleend aan het hoofd van de dienst. De inhoud van dit verzoek dient te voldoen aan het bepaalde in artikel 24, zesde lid, van het wetsvoorstel. Zo zal in het verzoek onder meer het onderzoek waarvoor de bevoegdheid moet worden ingezet dienen te worden omschreven alsmede het doel wat met de bevoegdheidsuitoefening wordt beoogd. Daarbij kan niet worden volstaan met een globale aanduiding, maar moet dit zo concreet als mogelijk is dienen te worden ingevuld. Op grond van artikel 33, derde lid, dient in het verzoek voorts een typering worden gegeven van de telecommunicatie of de gegevensoverdracht. Uit het verzoek moet bijvoorbeeld blijken of het gaat om interceptie van etherverkeer dan wel kabelgebonden telecommunicatie. Voorts zal de aard van het verkeer, zoals GSM-, radio- of internetverkeer, kunnen worden aangegeven al dan niet met een geografische afbakening. Ook zullen de diensten waar mogelijk opnemen welke soorten verkeer relevant zijn, zoals spraak, chatverkeer of bestandsuitwisseling. Waar het gaat om kabelgebonden telecommunicatie zal nader aangegeven dienen te worden welk deel van de kabelinfrastructuur het betreft en wat voor soort verkeer dient te worden geïntercepteerd. Evenals bij iedere andere bijzondere bevoegdheid, zal ook met betrekking tot de uitoefening van deze bevoegdheid een toets aan de eisen van

noodzakelijkheid, proportionaliteit en subsidiariteit dienen plaats te vinden (zie de artikelen 17, 43 en 44 van het wetsvoorstel). De toestemming kan ingevolge artikel 33, tweede lid, worden verleend voor een periode van ten hoogste twaalf maanden en kan telkens op een daartoe strekkend verzoek worden verlengd. Hiermee wordt afgeweken van de reguliere termijn van drie maanden, maar deze is gelet op het feit dat de indringendheid van de privacy-inbreuk in deze fase beperkt is en voorts de onderzoeksopdrachten voor een periode van een jaar worden vastgelegd, aangewezen.

In artikel 33, vierde lid, is bepaald dat de minister bevoegd is tot het verlenen van toestemming aan door hem bij besluit aangewezen aan hem ondergeschikte ambtenaren, welke ter uitvoering van het bepaalde in dit artikel – het gaat dan om het kennisnemen van de gegevens ten behoeve van de in het eerste lid, tweede volzin, genoemde activiteiten – bij uitsluiting van anderen kennis mogen nemen van de ingevolge artikel 33, eerste lid, verworven gegevens. Op deze wijze wordt geborgd dat de kennis die omtrent de (inhoud van de) gegevens wordt opgedaan in deze fase, niet zonder dat wordt voldaan aan de eisen gesteld aan de uitoefening van de bevoegdheden in de andere fasen voor (verdere) verwerking in die fasen beschikbaar komt (compartimentering).

Tot slot is in artikel 33, vijfde lid, van het wetsvoorstel voorzien in een bewaartermijn van drie jaren ten aanzien van de ingevolge het eerste lid verworven gegevens. Ook het huidige artikel 27, negende lid, Wiv 2002 kent een bewaartermijn, zij het dat die is gekoppeld aan de bevoegdheid tot (nadere) selectie en is beperkt tot een periode van een jaar. Deze termijn wordt in de praktijk van de diensten al jaren als een groot knelpunt ervaren. Ook de CTIVD heeft in het verleden in rapport nr. 3A (2005) inzake het onderzoek naar de rechtmatigheid van het MIVD-onderzoek naar proliferatie van massavernietigingswapens en overbrengingsmiddelen deze problematiek gesignaleerd. Teneinde deze problematiek te ondervangen wordt in het wetsvoorstel een termijn van drie jaren voorgesteld.[54] De gegevens worden bewaard voor een gegevensverwerking als bedoeld in artikel 34 en 35.[55] Gegevens waarvan in die periode is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel niet op hun relevantie van het onderzoek zijn onderzocht, dienen na afloop van de termijn van drie jaren te worden vernietigd. Onder relevant voor het onderzoek wordt verstaan: relevant voor het onderzoek waarvoor de toestemming is verleend en in welk kader de gegevens aldus zijn

[54] In het ingetrokken post-Madridwetsvoorstel was deze termijnverlenging ook reeds opgenomen; zie Kamerstukken I 2007/08, 30 553, a, Artikel I, onderdeel M.

[55] Overigens wordt opgemerkt dat – evenals nu het geval is met betrekking tot de gegevens die op grond van artikel 27, eerste lid, Wiv 2002 zijn verworven – met betrekking tot de ingevolge artikel 33, eerste lid, verworven gegevens, verstrekking in ongeëvalueerde vorm (veelal in bulk) aan buitenlandse collegadiensten – onder de daarvoor geldende voorwaarden en mits daarvoor toestemming van de voor de dienst verantwoordelijke minister is verkregen – kan plaatsvinden.

verworven. Voor de gegevens waarvan de versleuteling nog niet ongedaan is gemaakt geldt, evenals thans het geval is, dat de periode van drie jaren pas aanvangt met ingang van het moment waarop de versleuteling ongedaan is gemaakt.

Fase 2: de voorbewerking van de geïntercepteerde communicatie (artikel 34)

De gegevens die op grond van artikel 33, eerste lid, zijn geïntercepteerd mogen verder worden verwerkt op de voet van het bepaalde in artikel 34 of 35. In deze fasen kan onder voorwaarden kennis worden genomen van de inhoud van de geïntercepteerde gegevens. Bij de voorbewerking (fase 2) gaat het in eerste instantie niet om kennisneming van de inhoud *om de inhoud*, maar om informatie te verzamelen waarmee in het bijzonder het interceptieproces in bredere zin kan worden geoptimaliseerd; in fase 3 (de verdere verwerking), waarbij (onder meer) selectie van gegevens plaatsvindt, gaat het juist wel om de inhoud van de gegevens en het vaststellen van de relevantie daarvan voor het onderzoek door de diensten.

Verkenning van de telecommunicatie: search gericht op interceptie

In artikel 34, eerste lid, aanhef en onder a en b, wordt allereerst de bevoegdheid geregeld die thans – zij het in een andere en beperktere vorm - in artikel 26 Wiv 2002 is neergelegd, te weten het verkennen van de communicatie ook wel aangeduid als *search* gericht op *interceptie.* Het huidige artikel 26 Wiv 2002 regelt niet alleen de bevoegdheid tot interceptie ten behoeve van de verkenning van communicatie, maar beperkt deze ook tot niet-kabelgebonden telecommunicatie die bovendien zijn oorsprong of bestemming in andere landen heeft. Deze twee beperkingen zijn in dit wetsvoorstel komen te vervallen, waarbij ten aanzien van de laatstgenoemde beperking nog het volgende wordt opgemerkt. Indertijd is deze beperking opgenomen omdat de *search*-activiteit zich primair richtte op HF-radioverkeer en SHF-verkeer (satellietverkeer), waarvan werd opgemerkt dat er geen relevant binnenlands gebruik van werd gemaakt.[56] Nu de interceptiebevoegdheid technologieonafhankelijk is geformuleerd en daarmee is uitgebreid tot het kabelgebonden domein en waar het gaat om internetverkeer een dergelijke beperking geen betekenis heeft, is de beperking geschrapt. IP-verkeer zoekt immers automatisch de efficiëntste route via internet, waarbij ook voor verkeer met oorsprong of bestemming in het binnenland de efficiëntste route via een buitenlands netwerk kan verlopen (vice versa).

Evenals de bestaande bevoegdheid strekt de bevoegdheid er in eerste instantie toe om het gebruik dat van telecommunicatienetwerken wordt gemaakt te verkennen, en wel door het vaststellen van de kenmerken en de aard van de telecommunicatie alsmede de

[56] Kamerstukken II 1999/2000, 25 877, nr. 9, blz. 23-24.

identiteit van de persoon of organisatie behorende bij een telecommunicatie. In dat kader mag van de inhoud van de telecommunicatie worden kennisgenomen. Dit is onder omstandigheden nodig om bijvoorbeeld tot identificatie van een persoon of organisatie te komen, maar ook om de aard – militair, civiel of andersoortig verkeer – vast te stellen. Van de resultaten van het onderzoek mag, indien dat noodzakelijk is voor een goede taakuitvoering, - evenals nu het geval is – aantekening worden gehouden (artikel 34, derde lid). Met het hiervoor geschetste onderzoek wordt inzicht in het gebruik van de telecommunicatienetwerken verkregen, dat enerzijds een beeld oplevert van het communicatielandschap dat ingeval van toekomstige activiteiten, zoals bijvoorbeeld een militaire missie in het buitenland, reeds eerste aanknopingspunten biedt voor het verwerven van een adequate informatiepositie door de inzet van de interceptiebevoegdheid, en anderzijds bij kan dragen aan een meer doelgerichte inzet van de interceptiebevoegdheid als bedoeld in artikel 33, eerste lid. Een voorbeeld van dit laatste is dat op basis van analyse van telecommunicatie die van een bepaalde satellietlink is geïntercepteerd kan worden vastgesteld of deze voor het desbetreffende onderzoek van een dienst relevante communicatie bevat en aldus deze in interceptie dient te worden gehouden of te worden bijgezet. Voorts zal de technische verkenning een dienst in staat stellen het communicatielandschap in potentiële crisis- en missiegebieden in kaart te brengen, opdat onder andere bij militaire operaties snel tot een adequate inzet van interceptiemiddelen kan worden overgegaan.

Voor de uitoefening van deze bevoegdheid, maar dat geldt evenzeer voor de andere, hierna te bespreken, bevoegdheden als bedoeld in artikel 34, eerste en tweede lid, is toestemming van de voor de desbetreffende dienst verantwoordelijke minister vereist (artikel 34, vierde lid). Deze kan worden verleend op een daartoe strekkend verzoek van het hoofd van de dienst en wordt verleend voor een periode van ten hoogste twaalf maanden en kan telkens op een daartoe strekkend verzoek worden verlengd. De inhoud van dit verzoek dient te voldoen aan de eisen van artikel 24, zesde lid, van het wetsvoorstel. In de praktijk zal veelal sprake zijn van een combinatie van een verzoek om toestemming tot interceptie op grond van artikel 33 en een verzoek voor onderzoek als bedoeld in artikel 34, eerste lid, in verband met het feit dat de ene bevoegdheid òndersteunend is aan de uitvoering van de ander; het betreft dan een zogenaamde combinatie-last. Dat laat onverlet dat voor de uitoefening van beide bevoegdheden een toereikende motivering moet worden verschaft, inclusief een toets aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit moet plaatsvinden.

Netwerkmonitoring

De bevoegdheid van artikel 34, eerste lid, aanhef en onder a, is in samenhang met de bevoegdheid van artikel 33, eerste lid, waar het gaat om kabelgebonden telecommunicatie, ook van wezenlijke betekenis voor de beoogde activiteiten van de beide diensten in het cyberdomein waar het gaat om netwerkmonitoring of netwerkdetectie. Artikel 33, eerste lid, geeft een regeling voor de daarvoor benodigde interceptie in het kabelgebonden domein en artikel 34, eerste lid, aanhef en onder a, biedt de mogelijkheid om vervolgens met betrekking tot dat deel van het kabelgebonden domein waarvoor door de minister toestemming is verleend, onderzoek te doen naar kenmerken van ongewenste activiteiten (bijv. signatures van malware) en naar verkeer dat ongebruikelijke afwijkingen vertoont (anomalie-detectie), welke wijst op een mogelijke dreiging voor de nationale veiligheid. Dergelijk onderzoek kan zowel offline als *online* plaatsvinden. In het eerste geval wordt een gegevensbestand van ingevolge artikel 33, eerste lid, geïntercepteerde gegevens, gevormd, waarop vervolgens onderzoek plaatsvindt. In het tweede geval wordt bijvoorbeeld door de inzet van DPI-apparatuur[57], *realtime* en *online* het dataverkeer geanalyseerd. De hier bedoelde netwerkmonitoring vindt door de diensten plaats ter uitvoering van de aan hen opgedragen (contra-) inlichtingentaak, welke zijn basis vindt artikel 8, tweede lid, onder a, onderscheidenlijk artikel 10, tweede lid, onder a en c, van het wetsvoorstel.

Voor het uitvoeren van netwerkmonitoring of netwerkdetectie in het kader van de aan de dienst opgedragen (contra-)inlichtingentaak, waarbij de bijzondere bevoegdheden van artikel 33 en 34 worden ingezet, geldt dat daarvoor op eenzelfde wijze als hiervoor is beschreven met betrekking tot het verkennen van de communicatie in het algemeen, de wettelijk voorgeschreven toestemming van de minister moet worden verkregen, waarbij aan de daaraan gestelde eisen wordt voldaan. Bij het verzoek om toestemming zal niet alleen zo concreet mogelijk moeten worden aangegeven voor welk onderzoek, welk deel van de kabelgebonden infrastructuur voor welk doel dient te worden onderzocht, maar ook zal duidelijk dienen te worden aangegeven waaruit dat onderzoek precies bestaat. Aangezien de activiteit netwerkmonitoring of netwerkdetectie (artikel 34, eerste lid) niet zonder de bevoegdheid tot kabelgebonden interceptie op grond van artikel 33, eerste lid, kan plaatsvinden, zal ook hier veelal sprake zijn van een combinatie-last.

Verkenning van telecommunicatie: search gericht op selectie

In artikel 34, tweede lid, van het wetsvoorstel wordt aan *search* gericht op *selectie* een expliciete wettelijke basis gegeven. Daarbij worden twee situaties onderscheiden. Allereerst het vaststellen van en verifiëren van selectiecriteria in relatie tot personen en organisaties die door de diensten worden onderzocht. In dat geval is in de verleende

[57] Deep Packet Inspection-apparatuur, waarmee het dataverkeer kan worden onderzocht.

toestemming tot selectie ex artikel 35, tweede lid, de persoon of organisatie waarop de selectie kan worden toegepast reeds aangeduid. In de bulk aan geïntercepteerde telecommunicatie kan vervolgens op zoek worden gegaan naar selectiecriteria die – mits (aansluitend) op de voet van artikel 35, derde lid, vastgesteld – voor het onderzoek van de diensten naar die personen of organisatie relevante gegevens kunnen opleveren. Daarnaast kunnen reeds vastgestelde selectiecriteria op hun bruikbaarheid worden beproefd door in de bulk aan geïntercepteerde telecommunicatie te bezien of deze relevante gegevens voor het onderzoek opleveren. Deze vorm van *search* gericht op selectie komt min of meer overeen met de door de CTIVD in rapport nr. 28 inzake de toepassing van Sigint door de MIVD geformuleerde eerste vorm van *search*, te weten het *searchen* van de bulk aan communicatie om te bepalen of met de selectiecriteria waarvoor toestemming is verkregen de gewenste informatie kan worden gegenereerd.[58] De tweede situatie die in artikel 34, tweede lid, wordt geregeld, betreft het in relatie tot lopende onderzoeken van de dienst identificeren van personen of organisaties welke in aanmerking komen voor onderzoek door een dienst. Deze vorm van *search* is min of meer vergelijkbaar met de door de CTIVD in eerder genoemd rapport geformuleerde tweede vorm van *search* gericht op selectie: het *searchen* van de bulk aan communicatie om potentiële 'targets' te identificeren of te duiden.[59] In deze situatie wordt aan de hand van gegevens uit lopende onderzoeken, zoals de identiteit van personen of organisaties die reeds in onderzoek staan of andersoortige gegevens (zoals telefoonnummers, IP-adressen, e-mailadressen e.d), bezien of aan de hand van de in bulk geïntercepteerde telecommunicatie daaraan personen of organisaties zijn te koppelen die mogelijk voor onderzoek door de dienst in aanmerking komen. Indien het inderdaad om personen of organisaties gaat die voor onderzoek in aanmerking komen, en het wenselijk is dat van de inhoud van de hen betreffende communicatie kennis wordt genomen, kunnen in verband met het onderzoek naar hen selectiecriteria worden vastgesteld, indien daarvoor overeenkomstig het bepaalde in artikel 35, tweede lid, toestemming is gegeven (artikel 34, zesde lid).

Voor de uitoefening van de hiervoor geschetste bevoegdheden is op grond van artikel 34, vierde lid, van het wetsvoorstel toestemming van de voor de desbetreffende dienst verantwoordelijke minister vereist. Deze kan worden verleend op een daartoe strekkend verzoek van het hoofd van de dienst en wel voor de duur van twaalf maanden. Dit verzoek dient te voldoen aan de eisen van artikel 24, zesde lid. De toestemming kan op een daartoe strekkend verzoek van het hoofd van de dienst worden verlengd.

[58] CTIVD rapport nr. 28, blz. 43.
[59] CTIVD rapport nr. 28, blz. 44.

Bij de uitoefening van de in artikel 34 geregelde bevoegdheden wordt kennis genomen van de inhoud van de ingevolge artikel 33 verworven gegevens. Gelet op de aard en inhoud van de gegevens, waarbij de persoonlijke levenssfeer van personen in het geding kan zijn, is een zorgvuldige omgang daarmee aangewezen. Ook moet worden geborgd dat een verdere verwerking van de gegevens voldoet aan de daaraan te stellen vereisten en dat gegevens waarvan in onderhavig kader wordt kennisgenomen onder voorbijgaan daarvan voor die verdere verwerking beschikbaar komen. In artikel 34, vijfde lid, is daartoe bepaald dat de voor de dienst verantwoordelijke minister bevoegd is tot het verlenen van toestemming aan door hem bij besluit aangewezen aan hem ondergeschikte ambtenaren, welke ter uitvoering van het bepaalde in dit artikel, bij uitsluiting van anderen kennis mogen nemen van de inhoud van de ingevolge artikel 33 verworven telecommunicatie ten behoeve van de in het eerste en tweede lid bedoelde activiteiten. Deze aanwijsbevoegdheid kan aan het hoofd van de dienst worden gemandateerd.

Zoals in artikel 34, derde lid, is bepaald, mag van de resultaten van het onderzoek als bedoeld in het eerste en tweede lid, indien dat noodzakelijk is voor een goede taakuitvoering van de dienst, aantekening worden gehouden. Deze resultaten – bijvoorbeeld dat een bepaalde satellietlink wel of niet relevant is voor interceptie, welke persoon of organisatie van een bepaald telecommunicatiekanaal gebruik maakt, gegevens inzake aangetroffen malware, mogelijk relevante selectiecriteria en dergelijke – kunnen uiteraard wel verder gebruikt worden voor het doel waarvoor deze zijn opgetekend. Dat betekent niet dat iedere medewerker van de desbetreffende dienst gerechtigd zou zijn tot kennisneming van deze resultaten, maar uitsluitend die medewerkers die daarvan in het kader van de aan hen opgedragen taakuitvoering kennis moeten nemen (*need to know*-principe).

Wordt bij het onderzoek als bedoeld in artikel 34, eerste of tweede lid, geconstateerd dat nadere kennisneming van de inhoud van de communicatie noodzakelijk is voor een goede taakuitvoering van de dienst, dan dient, voor zover van toepassing, een verzoek om toestemming als bedoeld in artikel 32, tweede lid, onderscheidenlijk artikel 35, tweede lid, te worden ingediend. Een voorbeeld van de eerste situatie is bijvoorbeeld dat bij het *searchen* op HF-frequenties gestuit wordt op telecommunicatie van een persoon of organisatie die in onderzoek is van een dienst. Indien men het noodzakelijk acht dat deze telecommunicatie vervolgens wordt geïntercepteerd, dan zal daartoe een verzoek om toestemming tot gerichte interceptie ex artikel 32, tweede lid, dienen te worden gedaan. De tweede situatie doet zich, zoals hiervoor al is geschetst voor, indien bij het *searchen* op de bulk aan telecommunicatie in verband met de toepassing van artikel 35 nieuwe personen of organisaties worden onderkend die in aanmerking komen voor onderzoek

door de dienst en men ter zake wil overgaan tot selectie van hen betreffende gegevens. In dat geval zal eerst toestemming als bedoeld in artikel 35, tweede lid, dienen te worden verkregen.

Fase 3: (verder) verwerken van de telecommunicatie (artikel 35)

Algemeen

In de derde fase vindt, zoals ook in de kabinetsreactie op het rapport van de commissie Dessens ter zake is aangegeven[60], de selectie van relevante telecommunicatie plaats en worden de geselecteerde gegevens gebruikt om inzicht te verwerven in de intenties, de capaciteiten en de gedragingen van personen en organisaties die onderwerp zijn van onderzoek. Tevens vindt in deze fase metadata-analyse plaats, welke gericht kan zijn op het identificeren van personen of organisaties. Artikel 35 van het wetsvoorstel biedt voor de hiervoor beschreven activiteiten het wettelijk kader.

Selectie van gegevens

Selectie van gegevens vindt plaats met het oogmerk om van de inhoud van de geselecteerde gegevens kennis te kunnen nemen en deze vervolgens op relevantie voor het onderzoek ten behoeve waarvoor de selectie heeft plaatsgevonden te toetsen. Relevant geachte informatie uit de onderzochte gegevens worden vervolgens in het desbetreffende onderzoek betrokken en komen – immers er is vastgesteld dat het hier voor de nationale veiligheid relevante gegevens betreft - ook beschikbaar voor andere onderzoeken van de dienst, indien de desbetreffende gegevens eveneens daarvoor relevant zijn te achten. Ingevolge artikel 33, vierde lid, blijven de (in bulk) geïntercepteerde gegevens voor een periode van ten hoogste drie jaren voor het selectieproces beschikbaar. Daarmee is het mogelijk om aan de hand van nader verworven kennis en inzichten in het desbetreffende onderzoek te komen tot nieuwe selectiecriteria, waarmee aan de hand van nieuw vastgestelde selectiecriteria op de bulk aan gegevens kan worden geselecteerd. Een kortere bewaartermijn kan, zeker nu onderzoeken van de diensten zich in het algemeen over vele jaren uitstrekken, een doeltreffende analyse van de verworven data ten behoeve van die onderzoeken in de weg staan. Verworven data die voorheen irrelevant werd geacht kan immers van groot belang worden door nieuwe omstandigheden, zoals bij het identificeren van een nieuw target, het onderkennen van een niet nucleaire staat die nu de ontwikkeling van kernwapens nastreeft of het identificeren van een individu als terrorist. Ook kan sprake zijn van onderzoeksopdrachten die het opbouwen van lange termijn normbeelden noodzakelijk maken, zodat de diensten in staat zijn op tijd afwijkingen van dat

[60] Kamerstukken II 2014/15, 33 820, nr. 4, blz. 4.

normbeeld te constateren. Voorbeelden vanuit de praktijk van beide diensten leert dat een bewaarperiode van drie jaar de diensten in voldoende mate in staat stelt de toebedeelde onderzoeksopdrachten op verantwoorde wijze in te vullen.

De bevoegdheid tot selectie is in de huidige wet in artikel 27, derde lid e.v. geregeld. De thans voorgestelde regeling wijkt in verschillende opzichten van de huidige regeling af. Zo wordt geen onderscheid meer gemaakt in de drie categorieën van selectiecriteria (gegevens betreffende de identiteit van een persoon dan wel organisatie, een nummer als bedoeld in artikel 1.1, onder bb, van de Telecommunicatiewet dan wel enig technisch kenmerk, en aan een nader omschreven onderwerp gerelateerde trefwoorden), zoals thans in artikel 27, derde lid, Wiv 2002 wel het geval is. Voorts is voor wat betreft de systematiek van het vaststellen van selectiecriteria aangesloten bij die welke thans geldt voor het vaststellen van trefwoorden die zijn gerelateerd aan een onderwerp. Dat ziet ook op de daarbij bestaande mogelijkheid om de vaststelling van de selectiecriteria in mandaat te doen plaatsvinden. In het thans bestaande systeem wordt onderscheid gemaakt tussen enerzijds selectie op gegevens betreffende de identiteit van een persoon dan wel organisatie alsmede een nummer of enig technisch kenmerk en anderzijds selectie op aan een nader omschreven onderwerp gerelateerde trefwoorden. Voor de eerste categorie is indertijd aangegeven dat daarbij hetzelfde regime zou moeten worden toegepast als is voorzien in artikel 25 Wiv 2002, aangezien hier ook op een vergelijkbare, gerichte wijze gegevens – met betrekking de persoon of organisatie of het nummer dan wel enig ander technisch kenmerk – worden verzameld. Deze vergelijking is echter bij nader inzien niet in alle opzichten valide. Bij de bevoegdheid ex artikel 25 Wiv 2002 (artikel 32 van het wetsvoorstel) vindt er *real time* en *online* interceptie plaats van *alle* telecommunicatie van de desbetreffende persoon of organisatie die via het in een last opgenomen nummer wordt afgewikkeld. Dat betreft een zware inbreuk op de persoonlijke levenssfeer van de betrokkene, meer in het bijzonder van diens telefoongeheim. Bij selectie is van een dergelijke vergaande inbreuk op de persoonlijke levenssfeer geen sprake; er wordt immers niet *real time* en *online* kennis genomen van alle telecommunicatie, maar slechts van die gegevens die gerelateerd aan genoemde kenmerken voorhanden zijn in een bulk aan geïntercepteerde gegevens. Bovendien zal dat veelal niet alle telecommunicatie van betrokkene betreffen, maar uitsluitend die telecommunicatie waarbij in het kader van het transport gebruik is gemaakt van het telecommunicatiekanaal waarop in bulk is geïntercepteerd. Gelet hierop is het alleszins te rechtvaardigen om in het nieuwe stelsel voor een ander toestemmingsregime te kiezen, waarbij uiteraard wel in toereikende waarborgen is voorzien.

In artikel 35, eerste lid, aanhef en onder a, is bepaald dat de diensten bevoegd zijn tot het selecteren van de gegevens die door de uitoefening van de bevoegdheid, bedoeld in

artikel 33, zijn verzameld. Voor de uitoefening van deze bevoegdheid is op grond van het tweede lid toestemming vereist van de voor de desbetreffende dienst verantwoordelijke minister. Deze wordt op een daartoe strekkend verzoek verleend aan het hoofd van de dienst voor een periode van ten hoogste drie maanden en kan telkens op een daartoe strekkend verzoek worden verlengd. Het verzoek om toestemming dient te voldoen aan de eisen van artikel 24, zesde lid, van het wetsvoorstel. Daarbij is het van belang om – mede gelet op het bepaalde in het derde lid – een voldoende afgebakende omschrijving te geven van het onderzoek waarvoor de toestemming tot selectie wordt gevraagd, enigszins vergelijkbaar met de omschrijving van de onderwerpen waarvoor thans op grond van artikel 27, vijfde lid, Wiv 2002 toestemming wordt gevraagd. Daaromtrent is in de wetsgeschiedenis aangegeven, dat deze zo specifiek en nauwkeurig mogelijk moeten zijn omschreven. De toestemming voor selectie kan worden gegeven voor een periode van ten hoogste drie maanden met de mogelijkheid van verlenging – op een daartoe strekkend verzoek – voor eenzelfde periode. De termijn van een jaar, die thans geldt voor selectie op trefwoorden gerelateerd aan onderwerpen (artikel 27, vijfde lid, Wiv 2002), komt dan ook te vervallen.

In artikel 35, derde lid, wordt aansluitend bepaald, dat *ter uitvoering* van de door de minister verleende toestemming als bedoeld in het tweede lid, gerelateerd aan het desbetreffende onderzoek (zoals in het verzoek om toestemming omschreven), selectiecriteria kunnen worden vastgesteld.[61] Het vaststellen van de selectiecriteria geschiedt door de voor de desbetreffende dienst verantwoordelijke minister of namens deze het hoofd; artikel 24, tweede lid, is daarbij van overeenkomstige toepassing verklaard, hetgeen betekent dat het hoofd van de dienst aan hem ondergeschikte ambtenaren bij schriftelijk besluit kan aanwijzen die de selectiecriteria namens hem kunnen vaststellen. Bij het vaststellen van de selectiecriteria dienen deze te worden voorzien van een toereikende motivering, dat wil zeggen toereikend voor het doel van de selectie in relatie tot het onderzoek waarvoor de selectie plaatsvindt. Tot slot is erin voorzien dat in het geval dat de toestemming tot selectie vervalt, de daaraan gerelateerde selectiecriteria dienen te worden verwijderd.

Metadata-analyse

Metadata zijn die gegevens van telecommunicatie, welke niet de inhoud van de telecommunicatie betreffen. Het gaat dan bijvoorbeeld om gegevens als de bij de telecommunicatie gebruikte nummers (zoals telefoonnummers, IP-adressen, e-mailadressen), de met betrekking tot een communicatiesessie vastgelegde start- en eindtijd (inclusief duur), de cell-id's van de masten waarmee contact is gezocht (ingeval

[61] Het betreft hier een uitvoeringshandeling en geen bijzondere bevoegdheid.

van mobiele telefonie) enz. Zowel de huidige wet als het onderhavige wetsvoorstel geeft de diensten de bevoegdheid om deze gegevens omtrent een *specifieke* gebruiker op te vragen; zie artikel 28 Wiv 2002 onderscheidenlijk artikel 39 van het wetsvoorstel. Dergelijke gegevens komen echter ook beschikbaar bij interceptie van telecommunicatie door de diensten, zoals bij de interceptie ex artikel 33, eerste lid. Het gaat in dit laatste geval dan om een grote hoeveelheid metadata met een veelsoortige samenstelling.

Metadata zijn van wezenlijk belang voor de diensten, omdat aan de hand daarvan bijvoorbeeld kan worden vastgesteld met wie iemand heeft gebeld of heeft ge-e-maild, en wanneer dat heeft plaatsgevonden, welke websites iemand heeft bezocht, waar iemand op een bepaald moment zich bevond (ingeval gebruik mobiele telefonie) e.d. Door analyse van deze gegevens, zeker indien die worden gecombineerd met gegevens uit andere bronnen, kan met betrekking tot een persoon een beeld worden verkregen omtrent zijn relatienetwerk, verplaatsingsgedrag e.d. Het is evident dat daarmee onder omstandigheden een grote inbreuk op iemands persoonlijke levenssfeer kan worden gemaakt. De CTIVD heeft in rapport nr. 38[62] dan ook aanbevolen om voor de verwerking van metadata een regeling in de wet op te nemen. Zowel in de reactie op het toezichtsrapport als in het kabinetsstandpunt naar aanleiding van het rapport van de commissie Dessens is de noodzaak van een wettelijke regeling ter zake onderschreven. In laatstgenoemd kabinetsstandpunt is aangegeven dat geïntercepteerde metadata kan worden onderworpen aan een louter technische metadata-analyse en aan een meer vergaande analyse, waarbij wordt beoogd subjecten te identificeren en zicht te krijgen op patronen (zoals hiervoor geduid). Daarbij is aangegeven dat laatstgenoemde vorm van metadata-analyse wettelijk zal worden vastgelegd en worden onderworpen aan de wettelijke vast te leggen eis van ministeriële toestemming. Ook zullen daarbij de eisen van doelgerichte inzet, noodzakelijkheid, subsidiariteit en proportionaliteit van toepassing zijn. Ook zal een bewaar- en vernietigingstermijn van toepassing zijn.

In het wetsvoorstel is aan het voorgaande uitwerking gegeven. In artikel 35, eerste lid, onder b, van het wetsvoorstel wordt aan de diensten de bevoegdheid toegekend tot het toepassen van geautomatiseerde data-analyse als bedoeld in artikel 47 ten aanzien van ingevolge artikel 33 verzamelde gegevens anders dan die welke de inhoud van de desbetreffende telecommunicatie betreft. Artikel 47 van het wetsvoorstel geeft in algemene zin een regeling voor de toepassing van geautomatiseerde data-analyse van de diensten; daarbij is onder andere in algemene zin bepaald ten aanzien van welke gegevensbestanden door de diensten geautomatiseerde data-analyse kan worden toegepast en welke vormen van gegevensverwerking (in ieder geval) daarbij kunnen

[62] Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD (5 februari 2014).

worden toegepast (artikel 47, eerste en tweede lid). Zo kunnen ingevolge artikel 47, tweede lid, gegevens (in gegevensbestanden): (a) op geautomatiseerde wijze onderling met elkaar worden vergeleken, dan wel in combinatie met elkaar worden vergeleken, (b) worden doorzocht aan de hand van profielen en (c) worden vergeleken met het oog op het opsporen van bepaalde patronen. Metadata-analyse is aan te merken als geautomatiseerde data-analyse; daarbij kunnen de hiervoor genoemde verwerkingsmethoden worden toegepast.

In artikel 35, vierde lid, is bepaald dat voor geautomatiseerde data-analyse voor zover deze gericht is op het identificeren van personen of organisaties, waarbij sprake is van een verwerking als bedoeld in artikel 47, tweede lid, onder a, b en c (zie hiervoor), de toestemming wordt verleend door de voor de desbetreffende dienst verantwoordelijke minister op een daartoe strekkend verzoek van het hoofd van de dienst. Dit verzoek dient te voldoen aan de eisen van artikel 24, zesde lid, en in aanvulling daarop dient (a) een aanduiding te worden gegeven van de toe te passen vorm van geautomatiseerde data-analyse als bedoeld in artikel 47, tweede lid, en (b) voor zover van toepassing een aanduiding van de gegevensbestanden die in de geautomatiseerde data-analyse worden betrokken. Wat dit laatste betreft wordt nog het volgende opgemerkt. De metadata die onder toepassing van de bevoegdheid ex artikel 33, eerste lid, zijn verworven, kunnen op zich zelf staand worden geanalyseerd zonder dat daarbij andersoortige bestanden worden betrokken; echter het is ook mogelijk, en dat zal veeleer de praktijk zijn, dat het bestand met metadata wordt gecorreleerd met ander gegevensbestanden die de diensten ter beschikking hebben. In dat geval zullen die andere bestanden in het verzoek om toestemming dienen te worden aangeduid. Dat is van belang, omdat – al naar gelang de soort gegevensbestanden – daarmee ook duidelijk is tot welk resultaat de desbetreffende analyse kan leiden, hetgeen van belang is bij de te verrichten toets aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. De toestemming kan worden verleend voor een periode van ten hoogste twaalf maanden en telkens op een daartoe strekkend verzoek voor eenzelfde periode worden verlengd. In het vierde lid is ten slotte bepaald dat voor metadata-analyse in andere gevallen als bedoeld in de eerste volzin van dit artikellid geen toestemming als bedoeld in artikel 24 vereist is.

Waar het gaat om de bewaar- en vernietigingstermijn met betrekking tot de metadata, wordt verwezen naar het bepaalde in artikel 33, vierde lid, en hetgeen daaromtrent eerder in deze memorie van toelichting ter zake is gesteld.

Tot slot is in artikel 35, vijfde lid, een met artikel 33, vierde lid, en 34, derde lid, vergelijkbare bepaling opgenomen. Kortheidshalve wordt verwezen naar de daarop gegeven toelichting.

Informatie- en medewerkingsplicht aanbieders van communicatiediensten bij de verwerving van telecommunicatie op grond van artikel 33

In paragraaf 3.2.2.7.3 van het wetsvoorstel wordt in verband met de (beoogde) toepassing van de bevoegdheid ex artikel 33, voorzien in een tweetal daaraan ondersteunende bevoegdheden van de diensten en daarmee corresponderende medewerkingsverplichtingen van de desbetreffende aanbieders van communicatiediensten. Artikel 36 ziet op het verkrijgen van informatie om toepassing te kunnen geven aan de bevoegdheid tot interceptie ex artikel 33, eerste lid, van het wetsvoorstel. Artikel 37 ziet op de medewerking van de desbetreffende aanbieder aan een verleende toestemming op grond van artikel 33, tweede lid. Deze bevoegdheden kunnen, gelet op de technologieonafhankelijke formulering van de nieuwe interceptiebevoegdheid, zowel aangewend worden ten aanzien van aanbieders van niet-kabelgebonden als kabelgebonden telecommunicatie.

De informatieplicht ex artikel 36

In artikel 36, eerste lid, van het wetsvoorstel wordt aan de diensten de bevoegdheid verleend zich te wenden tot een aanbieder van communicatiediensten met het verzoek gegevens te verstrekken, welke noodzakelijk zijn om uitvoering te kunnen geven aan de bevoegdheid als bedoeld in artikel 33, eerste lid, van het wetsvoorstel. Het gaat hierbij om het verkrijgen van informatie die bij kan dragen aan het in kaart brengen van het communicatielandschap[63], welke noodzakelijk is om op enig moment uitvoering te kunnen geven aan de interceptiebevoegdheid van artikel 33. Voorts strekt artikel 36, eerste lid, ertoe om informatie te verkrijgen die nodig is om een verzoek om toestemming tot interceptie als bedoeld in artikel 33, tweede lid, adequaat te kunnen formuleren en – in het verlengde daarvan – de omschrijving van de medewerking die van de aanbieder van de communicatiedienst wordt verlangd.

Het in kaart brengen van het communicatielandschap is noodzakelijk om de interceptiebevoegdheid ex artikel 33, eerste lid, 'doelgericht' in te kunnen zetten. Daartoe is het noodzakelijk om zo goed mogelijk inzicht te verkrijgen wie waar welke soort telecommunicatie verwerkt c.q. transporteert; voorts dient de mogelijkheid voorhanden te zijn om van relevante aanbieders van communicatiediensten informatie te verkrijgen over de partijen waarmee zij overeenkomsten hebben afgesloten omtrent het

[63] Om doelgericht te kunnen intercepteren dient inzichtelijk te zijn waar, welke soort communicatie wordt verwerkt c.q. getransporteerd. Het betreft hier bijvoorbeeld informatie aangaande zakelijke klanten/(ver)huurders en regulier binnen de bedrijfsvoering van aanbieders van communicatiediensten bekende gegevens over de aangeboden diensten, karakteristieke van verkeersstromen en de belegging van communicatiekanalen.

gebruik van de door hen aangeboden netwerken en diensten.[64] Dit inzicht kan deels worden verkregen via uitoefening van de bevoegdheid ex artikel 34, eerste lid, van het wetsvoorstel tot verkenning van de telecommunicatie; een deel van de informatie zal echter uitsluitend van de desbetreffende aanbieders zelf kunnen worden verkregen. Aan de hand van die gegevens kunnen de diensten in relatie tot door hen verrichte onderzoeken bepalen welke aanbieders van communicatiediensten voor hen relevante communicatie afwikkelen. De informatieplicht strekt zich bovendien uitsluitend uit tot de gegevens die zij ten behoeve van de eigen bedrijfsvoering verwerken; er is met andere woorden geen sprake van een vergaarplicht. Voorts is de bevoegdheid om gegevens als bedoeld in artikel 36, eerste lid, eerste volzin op te vragen beperkt tot die categorieën van gegevens die bij algemene maatregel van bestuur zijn aangewezen.

Naast het verkrijgen van gegevens voor het in kaart brengen van het communicatielandschap, zullen, indien eenmaal is bepaald welke aanbieder relevante communicatie afwikkelt waarvoor de concrete toepassing van de bevoegdheid tot interceptie wordt overwogen, vervolgens gegevens dienen te worden verkregen die noodzakelijk zijn voor het opstellen van een verzoek om toestemming tot interceptie alsmede om uiteindelijk de medewerkingsplicht van de aanbieder zo nauwkeurig mogelijk te formuleren. Het gaat dan om onder meer de technische gegevens van bijvoorbeeld het door de desbetreffende aanbieder geëxploiteerde telecommunicatienetwerk en de daarbij aangewende apparatuur e.d., welke noodzakelijk zijn om – mede in overleg met de desbetreffende aanbieder – te kunnen bepalen welke technische voorzieningen er getroffen dienen te worden om feitelijk uitvoering te kunnen geven aan een verleende toestemming tot interceptie. In de eerder genoemde algemene maatregel van bestuur zullen ook de hier bedoelde categorieën van gegevens en wel in relatie tot het doen van een verzoek om toestemming als bedoeld in artikel 33, tweede lid, limitatief worden aangewezen.

In artikel 36, tweede lid, van het wetsvoorstel is bepaald dat voor het doen van een verzoek om gegevens te verstrekken geen toestemming is vereist als bedoeld in artikel 24. Er is daarvan afgezien, aangezien bij de gegevens waarop het verzoek betrekking heeft niet gaat om gegevens, waarbij de persoonlijke levenssfeer van concrete personen

[64] In zijn essentie vergelijkbaar met die welke in het kader van gerichte interceptie ex artikel 32 van het wetsvoorstel wordt toegepast, waarbij de diensten eveneens de bevoegdheid hebben om informatie over een bepaalde persoon of organisatie bij de aanbieders op te vragen, welke benodigd kan zijn om mede aan de hand daarvan te bepalen (a) *of* op de desbetreffende persoon of organisatie een gerichte interceptie dient plaats te vinden en (b) tot welke aanbieder(s) het verzoek om medewerking dient te worden gericht. Bij de onderhavige bevoegdheid zal het echter gelet op de aard van de diensten, te weten datatransport (en daaraan gerelateerde diensten), met name gaan om informatie betreffende de partijen die ter zake met de aanbieder een overeenkomst hebben afgesloten en waarover zij bedrijfsmatig de beschikking hebben.

in het geding is. Het gaat hierbij voornamelijk om technische en bedrijfsmatige gegevens die zicht bieden in hoe en waar communicatie verloopt. Dit heeft bijvoorbeeld betrekking op de fysieke en logische inrichting van netwerken, routering en signaaleigenschappen. Het verzoek wordt schriftelijk gedaan door het hoofd van de dienst en dient ten minste de volgende gegevens te bevatten: (a) gegevens betreffende de identiteit van de aanbieder van een communicatiedienst die de gegevens dient te verstrekken, (b) een omschrijving van de gegevens die dienen te worden verstrekt en (c) een redelijke termijn waarbinnen de gegevens dienen te worden verstrekt. Het spreekt voor zich dat ter zake van deze termijn er overleg met de aanbieder plaatsvindt.

De aanbieder aan wie een verzoek om gegevensverstrekking is gericht, is ingevolge artikel 36, vierde lid, verplicht aan het verzoek te voldoen. Het niet voldoen aan een dergelijk verzoek is in artikel 132 van het wetsvoorstel strafbaar gesteld. Op de verstrekking van de gegevens is artikel 22, vierde lid, van overeenkomstige toepassing verklaard. Dat betekent dat bij of krachtens de wet geldende voorschriften voor de verantwoordelijke voor een gegevensverwerking betreffende de verstrekking van zodanige gegevens niet van toepassing zijn op verstrekkingen die door de aanbieder naar aanleiding van een verzoek als bedoeld in artikel 36, eerste lid, worden gedaan. Voor een nadere toelichting op artikel 22, vierde lid, wordt verwezen naar hetgeen daaromtrent is gesteld in paragraaf 3.3.2 van deze memorie van toelichting.

Tot slot is in artikel 36, zesde lid, bepaald dat op het voldoen aan een verzoek artikel 13.6, tweede en derde lid, Tw van overeenkomstige toepassing is. Deze bepaling geeft een regeling voor de vergoeding van de door de aanbieder gemaakte kosten. Ingevolge artikel 13.6, tweede lid, komen voor vergoeding in aanmerking de door een aanbieder gemaakte administratiekosten en personeelskosten rechtstreeks voortvloeiend uit het voldoen aan een verzoek. Het derde lid van artikel 13.6 Tw voorziet in de mogelijkheid dat bij ministeriële regeling regels worden gesteld met betrekking tot de vaststelling van de kosten als bedoeld in het tweede lid.

De medewerkingsplicht ex artikel 37

Naast de bevoegdheid om met het oog op de (mogelijke) toepassing van artikel 33 informatie te vragen aan daarvoor in aanmerking komende aanbieders van communicatiediensten en een daarmee corresponderende verplichting om die informatie te verstrekken, wordt aansluitend in artikel 37 voorzien in de bevoegdheid om aan de desbetreffende aanbieder van een communicatiedienst medewerking te vragen bij de uitvoering van een ingevolge artikel 33, tweede lid, verleende toestemming tot interceptie van telecommunicatie; ook hier rust op de aanbieder een medewerkingsverplichting. Hoewel de in artikel 37 neergelegde

medewerkingsverplichting primair van belang is bij de uitoefening van de in artikel 33, eerste lid, neergelegde bevoegdheid tot interceptie met betrekking tot kabelgebonden telecommunicatie, is – door de technologieonafhankelijke formulering van de bevoegdheid van artikel 33 – deze echter ook in te roepen met betrekking tot daarvoor in aanmerking komende aanbieders bij de interceptie van niet-kabelgebonden telecommunicatie. Interceptie op de kabelgebonden infrastructuur zal echter uitsluitend met medewerking van de desbetreffende aanbieder van communicatiediensten plaatsvinden. Van een onbeperkte en zelfstandige toegang van de diensten tot de kabelgebonden telecommunicatie-infrastructuur is derhalve geen sprake. De plicht tot medewerking is geregeld in artikel 13.2 Tw[65] voor zover de medewerking wordt ingeroepen van aanbieders van openbare telecommunicatienetwerken en –diensten en in artikel 37, vijfde lid, voor de overige aanbieders van communicatiediensten.

De uitoefening van de in artikel 37, eerste lid, geregelde bevoegdheid is uitsluitend toegestaan, indien door de voor de desbetreffende dienst verantwoordelijke minister op een daartoe strekkend verzoek aan het hoofd van de dienst toestemming is verleend. De toestemming wordt verleend voor een periode van ten hoogste twaalf maanden en kan telkens op een daartoe strekkend verzoek voor eenzelfde periode worden verlengd (artikel 37, derde lid). Deze toestemming is dus vereist naast de toestemming die ingevolge artikel 33, tweede lid, voor de interceptie als zodanig is vereist. Dat is een afwijking van het systeem dat voor de in artikel 32, eerste lid, neergelegde bevoegdheid tot gerichte interceptie is neergelegd, waarbij de verleende toestemming tevens de verplichting tot medewerking ex artikel 13.2 Tw constitueert. Een afzonderlijke toestemming om de medewerking van een aanbieder bij de uitoefening van de bevoegdheid ex artikel 33, eerste lid, van het wetsvoorstel in te roepen, is vereist, omdat daarbij tevens dient te worden vastgesteld welke soort medewerking van de aanbieder wordt verlangd (maatwerk). Anders dan bij gerichte interceptie op grond van artikel 32, eerste lid, waar bij uitvoering van de verleende toestemming in de regel de medewerking is vereist van een aanbieder van openbare telecommunicatienetwerken of –diensten en die op grond van artikel 13.1 Tw reeds op voorhand (technisch) aftapbaar dienen te zijn overeenkomstig hetgeen in het Besluit aftappen openbare telecommunicatienetwerken en –diensten en de Regeling aftappen openbare telecommunicatienetwerken en -diensten is gesteld, geldt bij de uitoefening van onderhavige bevoegdheid dat hier maatwerk is vereist. Bovendien komen voor de medewerking bij de uitoefening van de in artikel 33,

[65] Artikel 13.2 Tw bepaalt *in algemene zin* dat aanbieders van openbare telecommunicatienetwerken- en diensten verplicht zijn om medewerking te verlenen aan de uitvoering van een toestemming op grond van de Wiv 2002 tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld onderscheidenlijk tot het aftappen of opnemen van door hen verzorgde telecommunicatie.

eerste lid, neergelegde bevoegdheid een beperkt aantal – en dus niet alle - aanbieders in aanmerking.

Het verzoek om toestemming dient in aanvulling op het bepaalde in artikel 24, zesde lid, gegevens te bevatten betreffende de identiteit van de aanbieder van een communicatiedienst wiens medewerking wordt verlangd en een nauwkeurige omschrijving van de soort medewerking welke van de desbetreffende aanbieder wordt verlangd. Voor dit laatste is het cruciaal om over de benodigde informatie te beschikken met betrekking tot de telecommunicatie-infrastructuur van de desbetreffende aanbieder; artikel 36 biedt de wettelijke basis om die informatie te verkrijgen en ook overigens zal vooruitlopend op een verzoek om toestemming als bedoeld in het tweede lid reeds met de desbetreffende aanbieder contact zijn om te bezien waaruit de verlangde medewerking zou moeten bestaan. Dat is niet alleen in belang van de dienst, maar ook van de desbetreffende aanbieder teneinde te verzekeren dat wat van hem verlangd wordt ook door hem uitvoerbaar is. Is de toestemming eenmaal door de minister verleend, dan wordt deze ingevolge het vierde lid, niet eerder ter uitvoering gebracht dan nadat ter zake met de desbetreffende aanbieder overleg is gevoerd. De in het verzoek om toestemming omschreven soort medewerking zal naar verwachting naar zijn aard niet alle details van de verlangde medewerking, bijvoorbeeld de precieze specificaties van de technische voorzieningen en dergelijke, bevatten. Het voorgeschreven nader overleg met de aanbieder is onder meer bedoeld om hieraan nader uitwerking te geven. Ook kan dan over andersoortige aangelegenheden als de implementatietermijn en eventuele personele en organisatorische aspecten verbonden aan de uitvoering van de verleende toestemming worden gesproken.[66] Mocht een verleende toestemming ongewijzigd worden verlengd en aldus ook geen wijziging optreden in de soort medewerking die van de aanbieder wordt verlangd, dan is het niet vereist om over de uitvoering daarvan opnieuw te overleggen (artikel 37, vierde lid). Overigens zal in de praktijk er regelmatig contact en overleg zijn tussen de diensten de betreffende aanbieders over de diverse aspecten van de tenuitvoerlegging van de verleende toestemming.

Zoals hiervoor reeds is aangegeven zal de uitvoering van de hier bedoelde interceptiebevoegdheid bij de desbetreffende aanbieder qua technische voorzieningen en dergelijke maatwerk vereisen, welke niet alleen de nodige implementatietijd maar ook de nodige investeringen vergt. Indien op enig moment, bijvoorbeeld als gevolg van wijziging in de onderzoeksopdrachten van de diensten, het niet meer noodzakelijk is om bij de desbetreffende aanbieder telecommunicatie te intercepteren op de voet van artikel 33,

[66] Zoals bijvoorbeeld de te nemen beveiligingsmaatregelen en het aanwijzen van vertrouwensfuncties.

eerste lid, en ter zake van hem de medewerking als bedoeld in artikel 37, eerste lid, in te roepen, is het niettemin wenselijk dat voor een beperkte periode, te weten twaalf maanden na afloop van een toestemming als bedoeld in artikel 37, tweede lid, de door hem getroffen voorzieningen van technische aard in stand te houden. Mocht in die periode nodig blijken om wederom de medewerking van de desbetreffende aanbieder in te roepen, dan kan deze op korte termijn worden gerealiseerd. Dat kan bijvoorbeeld aan de orde zijn, indien door een acute (internationale) crisissituatie de voor (de verwerking van) interceptie beschikbare capaciteit bij de diensten als gevolg van een herprioritering tijdelijk voor een ander onderzoek en bij een andere aanbieder moest worden ingezet, maar daarna met betrekking tot de door de desbetreffende aanbieder afgewikkelde telecommunicatie weer kan worden opgepakt; hiermee wordt tevens een onnodige desinvestering aan de kant van de aanbieder voorkomen.

Tot slot is in artikel 37, zevende lid, bepaald dat artikel 13.6 Tw van overeenkomstige toepassing is verklaard op de verlangde medewerking van de aanbieder. Artikel 13.6 Tw geeft – voor zover hier relevant - een regeling voor de toedeling van kosten die door aanbieders van openbare telecommunicatienetwerken en –diensten dienen te worden gemaakt in verband met het (onder meer) het aftapbaar maken van hun netwerken en diensten, alsmede het voldoen aan een verleende toestemming tot het aftappen en opnemen op grond van de Wiv 2002. De investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen voor het aftapbaar maken van netwerken en diensten komen ingevolge artikel 13.6, eerste lid, Tw voor rekening van de desbetreffende aanbieder. Op grond van artikel 13.6, tweede lid, hebben de aanbieders van openbare telecommunicatienetwerken en –diensten aanspraak op vergoeding uit ’s-Rijks kas van de door hen gemaakte administratiekosten en personeelskosten rechtstreeks voortvloeiend uit het voldoen van een verleende toestemming op grond van de Wiv 2002. Er is vooralsnog geen aanleiding om waar het gaat om de medewerking aan de uitvoering van de bevoegdheid tot interceptie als bedoeld in artikel 33, eerste lid, te voorzien in een hiervan afwijkende regeling inzake kostentoedeling.

3.3.3.4.7.5 Informatieverzoeken en medewerkingsplicht met betrekking tot telecommunicatiegegevens

In paragraaf 3.2.2.7.5 van het wetsvoorstel worden een drietal bevoegdheden van de diensten geregeld waar het gaat om het opvragen van telecommunicatiegegevens bij aanbieders van communicatiediensten. Twee van de drie bevoegdheden, te weten die welke zijn neergelegd in de artikelen 39 en 40, komen – zij het in aangepaste vorm – in de plaats van de bestaande bevoegdheden van de diensten tot het opvragen van verkeersgegevens (artikel 28 Wiv 2002) en het opvragen van abonneegegevens (artikel

29 Wiv 2002).[67] De bevoegdheid in artikel 38 van het wetsvoorstel is nieuw en ziet op het opvragen van bij een aanbieder van een communicatiedienst opgeslagen telecommunicatie van een gebruiker.

Het opvragen van bij een aanbieder van een communicatiedienst opgeslagen telecommunicatie van een gebruiker (artikel 38)

Sinds de inwerkingtreding van de Wiv 2002 in 2002, hebben er zich op het vlak van de informatie- en communicatietechnologie (ICT) forse ontwikkelingen voorgedaan die onmiskenbaar gevolgen hebben voor de mogelijkheden van de inlichtingen- en veiligheidsdiensten om in het kader van de uitvoering van hun wettelijk opgedragen taken de daarvoor vereiste gegevens te verkrijgen. Niet alleen wordt, zoals eerder geschetst, het gros van de telecommunicatie tegenwoordig via de kabelgebonden telecommunicatie-infrastructuur afgewikkeld, maar ook nemen ICT-diensten in toenemende mate hun toevlucht tot de *cloud*.[68] Dat betekent dat de voor de inlichtingen- en veiligheidsdiensten relevante gegevens steeds minder in de fysieke nabijheid van hun onderzoekssubjecten aanwezig zijn, maar 'ergens' in de *cloud*. Op dit moment hebben de diensten niet de bijzondere bevoegdheid om bij aanbieders van communicatiediensten, waaronder begrepen de cloud-dienstverleners, gegevens van gebruikers van die diensten op te vragen die door deze aanbieders als onderdeel van de door hen verleende communicatiedienst worden opgeslagen. Weliswaar bestaat de mogelijkheid om op grond van artikel 17 Wiv 2002 (artikel 20 van het wetsvoorstel) de aanbieder om de verstrekking van dergelijke gegevens te verzoeken, echter deze is niet verplicht om aan een dergelijk verzoek gehoor te geven. Dit is een onwenselijke situatie, zeker nu veel personen en organisaties waar de diensten onderzoek naar verrichten van *cloud*-diensten gebruik maken en ingeval hiervoor niet in een toereikende en effectieve bevoegdheid wordt voorzien, er onmiskenbaar sprake zal zijn van een verslechtering van de informatiepositie en de onderzoeksmogelijkheden van de diensten. Dit is gelet op het belang van de nationale veiligheid een onwenselijke situatie, waarvoor een adequate voorziening moet worden getroffen. Artikel 38 voorziet daarin.

Op grond van artikel 38, eerste lid, van het wetsvoorstel zijn de diensten bevoegd zich te wenden tot een aanbieder van een communicatiedienst met het verzoek gegevens te

[67] In het ingetrokken post-Madridwetsvoorsel was reeds in een vergelijkbare aanpassing voorzien; zie Kamerstukken I 2007/08, 30 553, A, Artikel I, onder N.
[68] De *cloud* is een begrip dat *online*diensten aanduidt. *Cloud computing* is het via internet op aanvraag beschikbaar stellen van hardware, software en gegevens. De *cloud* ("wolk") staat voor een netwerk dat met al de computers die erop zijn aangesloten een soort "wolk" van computers vormt, waarbij de eindgebruiker niet weet op hoeveel of op welke computer(s) software draait, gegevens zijn opgeslagen of waar die computers zich bevinden. Het gebruikmaken van de cloud is inmiddels de normaalste aak van de wereld; van de 8,5 miljoen smartphones in Nederland maakt een groot gedeelte gebruik van *cloud*-diensten voor e-mail en data-opslag.

verstrekken die betrekking hebben op de telecommunicatie van een gebruiker die door de aanbieder als onderdeel van de door hem verleende communicatiedienst ten behoeve van een gebruiker is opgeslagen. De medewerkingsplicht voor de aanbieder is in het vierde lid neergelegd. Het gaat hierbij, anders dan bij de in artikel 39 en 40 geregelde bevoegdheid, om gegevens betreffende de inhoud van de telecommunicatie. Daarbij moet onder meer worden gedacht aan de inhoud van een mailbox van een gebruiker die in het kader van de door de aanbieder verleende webmaildienst bij hem is opgeslagen, de bij een aanbieder opgeslagen voicemail van de gebruiker, en de door een aanbieder van data-opslagdiensten bij hem opgeslagen gegevens van een gebruiker. Bij algemene maatregel van bestuur zullen met betrekking tot daarin aangeduide categorieën van communicatiediensten de categorieën van gegevens worden aangewezen waarop het verzoek betrekking kan hebben.

Voor de uitoefening van deze bevoegdheid is de toestemming van de voor de dienst verantwoordelijke minister nodig, die deze op een daartoe strekkend verzoek kan verlenen aan het hoofd van de dienst. De toestemming is hier op het niveau van de minister gelegd, aangezien het hier gaat om gegevens betreffende de inhoud van telecommunicatie, waarvoor in het geval dat deze in “stromende” vorm zouden worden verkregen – namelijk door toepassing van de bevoegdheid tot gerichte interceptie ex artikel 32 van het wetsvoorstel – dan wel via het binnendringen in een geautomatiseerd werk van het onderzoekssubject – zie artikel 30 van het wetsvoorstel - ook de toestemming van de minister is vereist. De zwaarte van de inbreuk op de persoonlijke levenssfeer is bij de toepassing van onderhavige bevoegdheid daarmee vergelijkbaar.

Het verzoek om toestemming wordt schriftelijk gedaan en bevat in aanvulling op hetgeen is bepaald in artikel 24, zesde lid, het nummer of een andere aanduiding waarmee de gebruiker kan worden geïdentificeerd, een nauwkeurige omschrijving van de gegevens die verstrekt moeten worden (en die in de algemene maatregel van bestuur als bedoeld in het eerste lid zijn aangewezen) alsmede de periode waarover de gegevens verstrekt dienen te worden.

In artikel 38, vijfde lid, is artikel 22, vierde lid, van overeenkomstige toepassing verklaard. Voor een toelichting ter zake wordt kortheidshalve naar de toelichting op artikel 22 verwezen. In het vijfde lid is vervolgens artikel 13.6, tweede en derde lid, Tw van overeenkomstige toepassing verklaard op het voldoen aan een verzoek als bedoeld in het eerste lid. Dat betekent dat de aanbieder recht heeft op vergoeding van de door hem in verband daarmee gemaakte administratiekosten en personeelskosten.

Tot slot is in artikel 38, zevende lid, een regeling opgenomen, die de diensten ertoe dwingt om de gegevens die zij door toepassing van onderhavige bevoegdheid van de

aanbieder hebben verkregen zo spoedig mogelijk te onderzoeken op hun relevantie voor het onderzoek waarvoor ze zijn verworven. Gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel niet op hun relevantie voor het onderzoek zijn onderzocht, dienen binnen een periode van ten hoogste twaalf maanden nadat zij zijn verworven te worden vernietigd.

Het opvragen van verkeersgegevens (artikel 39)

In artikel 39 van het wetsvoorstel is een regeling gegeven voor het opvragen van zogeheten verkeersgegevens (ook wel metadata) bij een aanbieder van een communicatiedienst. Op dit moment is deze bevoegdheid geregeld in artikel 28 Wiv 2002. Ten opzichte van de bestaande regeling is de regeling zoals voorzien in het wetsvoorstel in enkele opzichten gewijzigd. Allereerst is de reikwijdte van de bevoegdheid verruimd in die zin dat deze kan worden uitgeoefend jegens de aanbieders van communicatiediensten; op dit moment is de uitoefening beperkt tot de aanbieders van openbare telecommunicatienetwerken en –diensten in de zin van de Tw. Voor de betekenis van het begrip aanbieder van een communicatiedienst wordt verwezen naar paragraaf 3.3.3.4.7.2 van deze memorie van toelichting. Voorts wordt de reikwijdte van de regeling in die zin verruimd dat niet alleen gegevens kunnen worden opgevraagd die gerelateerd zijn aan een nummer of een specifieke gebruiker, maar ook die gerelateerd zijn aan een gespecificeerde locatie (zie het derde lid, onder b). Het gaat hier om het opvragen van zogeheten 'mastgegevens'. Het opvragen van mastgegevens door de AIVD en MIVD stelt de diensten in het kader van hun operationele onderzoeken, bijvoorbeeld in het kader van contra-terrorisme, in staat (mobiele communicatieapparatuur in gebruik bij) targets van de diensten aan relevante locaties te linken. Met de analyse van de mastgegevens kan in geval van een aanslag, incident of een heimelijke ontmoeting inzicht verkregen worden welke communicatieapparatuur op het moment van de aanslag, het incident of ontmoeting in de buurt aanwezig waren, en daarmee mogelijk ook het target.[69] Ten derde wordt in het tweede lid bepaald dat voor de uitoefening van de bevoegdheid toestemming is vereist van de minister of namens deze het hoofd van de dienst; er bestaat geen mogelijkheid om deze bevoegdheid door te mandateren. Hiermee wordt in tegenstelling tot de huidige regeling, waarbij geen toestemmingsvereiste is gesteld, voorzien in een extra waarborg. Tot slot is de thans in artikel 28, vijfde lid, Wiv 2002 opgenomen deconflictieregeling komen te vervallen; de in artikel 75 van het wetsvoorstel opgenomen regeling treedt daarvoor in de plaats.

[69] Volledige zekerheid dat het target in de buurt was is hier overigens niet uit af te leiden, omdat de communicatie-apparatuur ook op de desbetreffende door een derde in gebruik kan zijn geweest.

De diensten zijn op grond van artikel 39, eerste lid, bevoegd om zich te wenden tot een aanbieder van een communicatiedienst met het verzoek gegevens te verstrekken over een gebruiker en het communicatieverkeer dat met betrekking tot die gebruiker voor of op het tijdstip van het verzoek heeft plaatsgevonden dan wel na dat tijdstip zal plaatsvinden. Indien de aanbieder toekomstige verkeersgegevens *real time* en *online* aan de dienst dient te verstrekken, wordt ook wel gesproken over een 'stomme tap'; de inhoud van de telecommunicatie wordt dan niet verstrekt. De gegevens die door de aanbieder dienen te worden verstrekt zullen, evenals nu het geval is, limitatief bij algemene maatregel van bestuur worden aangewezen. De huidige regeling ter zake, het besluit ex artikel 28 Wiv 2002, zal tezijnertijd aan de nieuwe regeling dienen te worden aangepast; daarbij zal worden gedifferentieerd naar de te onderscheiden categorieën van communicatiediensten (zoals aanbieders van vaste telefoondiensten, van mobiele telefoondiensten, van internet, webhosts e.d).

Het verzoek om toestemming tot uitoefening van de bevoegdheid als bedoeld in het tweede lid, dient te voldoen aan de eisen van artikel 24, zesde lid. Dit verzoek dient te worden onderscheiden van het verzoek dat aan de aanbieder wordt gericht en waarvoor het derde lid regels stelt. Het verzoek aan de aanbieder dient de volgende gegevens te bevatten: (a) het nummer of een andere aanduiding waarmee de gebruiker kan worden geïdentificeerd of (b) gegevens betreffende de locatie van de gebruiker, en (c) een omschrijving van de gegevens die verstrekt dienen te worden, alsmede (d) de periode waarover de gegevens moeten worden verstrekt.

In artikel 39, vierde lid, is een aanvullende voorziening getroffen voor die aanbieders van communicatiediensten, die geen aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst zijn, waar het gaat om de plicht tot medewerking aan een verzoek als bedoeld in het eerste lid. Voor aanbieders van openbare telecommunicatienetwerken en –diensten als bedoeld in de Telecommunicatiewet is in artikel 13.4, eerste lid, Tw reeds in een medewerkingsplicht voorzien. Het niet voldoen aan een verzoek tot medewerking als bedoeld in artikel 39, vierde lid, is in artikel 132 van het wetsvoorstel strafbaar gesteld.

In artikel 39, zesde lid, is ten slotte voor die aanbieders van communicatiediensten, waarop niet reeds artikel 13.6 Tw van toepassing is, artikel 13.6, tweede en derde lid, van overeenkomstige toepassing verklaard. Dat betekent dat deze aanspraak hebben op vergoeding uit 's Rijks kas van de door hen gemaakte administratiekosten en personeelskosten die rechtstreeks voortvloeien uit het voldoen aan een verzoek om gegevensverstrekking als bedoeld in artikel 39, eerste lid.

De verstrekking van gebruikersgegevens (artikel 40)

Artikel 40 geeft een regeling voor het opvragen van gebruikersgegevens[70] bij een aanbieder van communicatiediensten. De desbetreffende gegevens zijn in het eerste lid limitatief opgesomd. Het betreft gegevens ter zake van (a) naam, adres, postcode, woonplaats, nummer en soort dienst van de gebruiker, alsmede (b) naam, adres, postcode, woonplaats van degene die de rekening betaalt voor de communicatiedienst die de gebruiker ter beschikking heeft of gehad en het daarvoor gebruikte bankrekeningnummer dan wel betalingsmiddel. Deze bevoegdheid komt overeen met de bestaande bevoegdheid ex artikel 29 Wiv 2002, doch is evenals bij de hiervoor besproken bevoegdheid tot het opvragen van verkeersgegevens qua reikwijdte uitgebreid tot aanbieders van communicatiediensten. Voorts is in het eerste lid, onder b, in aanvulling op het gebruikte bankrekeningnummer erin voorzien dat ook gegevens omtrent andere betalingsmiddelen moeten worden verstrekt; met deze aanvulling wordt beoogd rekening te houden met toekomstige ontwikkelingen, zoals betalingen met *bitcoin*.

Evenals nu is voor de uitoefening van de bevoegdheid geen toestemming vereist als bedoeld in artikel 24, eerste lid.

In artikel 13.4, tweede lid, Tw is de medewerkingsplicht voor de aanbieders van openbare telecommunicatienetwerken en –diensten neergelegd met betrekking tot een verzoek als hiervoor bedoeld. Op grond van artikel 13.4, vierde lid, Tw is het Besluit verstrekking gegevens telecommunicatie vastgesteld, waarin een regeling is getroffen voor de verstrekking van de desbetreffende informatie door tussenkomst van het Centraal informatiepunt onderzoek telecommunicatie (CIOT). Dat is een volledig geautomatiseerd proces, waarbij de hier bedoelde aanbieders de in genoemd besluit aangeduide gegevens – die dagelijks dienen te worden geactualiseerd – ter beschikking stelen aan het CIOT en de daartoe geautoriseerde medewerkers van de diensten deze gegevens via het CIOT bevragen. Voor andere aanbieders van communicatiediensten dan de aanbieders van openbare communicatienetwerken en – diensten als bedoeld in de Tw geldt dit stelsel niet; hoofdstuk 13 Tw (Bevoegd aftappen en toepassing van andere bevoegdheden op grond van het Wetboek van Strafvordering en de Wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met telecommunicatie) is niet op hen van toepassing. Vandaar dat in artikel 40, vierde, vijfde en zevende lid ter zake van deze andere aanbieders voorzien is in een aanvullende regeling. In het vierde lid is de medewerkingsplicht voor deze aanbieders neergelegd. In het vijfde lid is bepaald dat een verzoek om verstrekking van de gegevens schriftelijk wordt gedaan door of namens het hoofd van de dienst. In het zevende lid is tot slot de in artikel 13.6, tweede en derde lid,

[70] Vergelijkbaar met abonneegegevens.

Tw opgenomen regeling inzake kostenvergoeding van overeenkomstige toepassing verklaard.

In artikel 40, derde lid, wordt aan de diensten voorts de bevoegdheid toegekend om, in het geval dat de gegevens als bedoeld in het eerste lid, onder a, niet bekend zijn bij de desbetreffende dienst, doch deze benodigd zijn om toepassing te kunnen geven aan artikel 32 (gerichte interceptie) en artikel 39 (opvragen verkeersgegevens), de aanbieder van een openbare telecommunicatienetwerk of een openbare telecommunicatiedienst als bedoeld in de Telecommunicatiewet te verzoeken deze gegevens te achterhalen en te verstrekken. In artikel 13.4, derde lid, Tw is – als spiegelbepaling – de medewerkingsplicht van de hier bedoelde aanbieders geregeld met betrekking tot een dergelijk verzoek. In artikel 13.4, vierde lid, Tw is aansluitend bepaald dat bij algemene maatregel van bestuur onder meer regels kunnen worden gesteld met betrekking tot de wijze waarop de aanbieders aan een dergelijk verzoek dienen te voldoen. De desbetreffende regels zijn waar het gaat om het achterhalen van het verlangde nummer door de aanbieder neergelegd in het Besluit bijzondere vergaring nummergegevens telecommunicatie, meer in het bijzonder paragraaf 3 (bestandsanalyse).

3.3.3.4.7.6 Medewerkingsplicht bij ontsleuteling van communicatie

In de artikelen 32, eerste lid, en 33, eerste lid, waarin de bevoegdheden tot interceptie (gericht onderscheidenlijk in andere gevallen) van de diensten zijn geregeld, is aan de diensten tevens de bevoegdheid gegeven tot het ongedaan maken van de versleuteling van gesprekken, telecommunicatie of gegevensoverdracht onderscheidenlijk telecommunicatie of gegevensoverdracht. Dat is een bestaande bevoegdheid (zie artikel 25, eerste lid, 26, eerste lid, en artikel 27, eerste lid Wiv 2002). Op dit moment is echter alleen in artikel 25, zevende lid, Wiv 2002 voorzien in een medewerkingsplicht bij ontsleuteling van communicatie: een ieder die kennis draagt ter zake van het ongedaan maken van de versleuteling van gespreken, telecommunicatie of gegevensoverdracht als bedoeld in artikel 25, eerste lid, Wiv 2002, is verplicht het hoofd van de dienst op diens schriftelijk verzoek alle noodzakelijke medewerking te verlenen om deze versleuteling ongedaan te maken. Het niet voldoen aan een verzoek om medewerking is in artikel 89, eerste lid, Wiv 2002 strafbaar gesteld. Ook in de andere genoemde gevallen dan artikel 25 Wiv 2002 is het echter wenselijk om, indien daartoe de noodzaak bestaat, de mogelijkheid te hebben een medewerkingsplicht op te kunnen leggen aan de kennisdragers met betrekking tot versleuteling.

In artikel 41 van het wetsvoorstel wordt aan de diensten de bevoegdheid toegekend om in het kader van de uitoefening van de bevoegdheid, bedoeld in de artikelen 32, eerste lid, tweede volzin, en 33, eerste lid, tweede volzin, zich te wenden tot degene van wie

redelijkerwijs vermoed wordt dat hij kennis draagt van de wijze van versleuteling van de desbetreffende gesprekken, telecommunicatie of gegevensoverdracht met het verzoek alle noodzakelijke medewerking te verlenen tot het ontsleutelen van de gegevens door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken. Bij het formuleren van deze bevoegdheid is aansluiting gezocht bij de formulering van een vergelijkbare bevoegdheid in artikel 126m, zesde lid, van het Wetboek van Strafvordering. In artikel 41, vierde lid, is de medewerkingsplicht neergelegd voor degene tot wie een verzoek als hier bedoeld wordt gericht. Het niet voldoen hieraan is in artikel 132 van het wetsvoorstel strafbaar gesteld.

Voor het uitoefenen van deze bevoegdheid is toestemming van de voor de desbetreffende dienst verantwoordelijke minister vereist (artikel 41, tweede lid). Het verzoek om toestemming is ingevolge het derde lid schriftelijk en dient in aanvulling op hetgeen in artikel 24, zesde lid, is bepaald voorts aan te geven van wie de medewerking wordt verlangd alsmede een omschrijving te bevatten van de gesprekken, telecommunicatie of gegevensoverdracht ten aanzien waarvan de medewerking wordt verlangd.

3.3.3.4.8 Toegang tot plaatsen

Voor de uitoefening van diverse bijzondere bevoegdheden door de diensten is toegang vereist tot plaatsen; dat is met name van belang waar het gaat om toegang tot besloten plaatsen waaronder begrepen woningen. Artikel 30 van de Wiv 2002 voorziet daar thans in. In artikel 42 van het wetsvoorstel wordt deze bevoegdheid opnieuw en in aangevulde vorm geregeld. In de praktijk is gebleken dat de bestaande formulering van de bevoegdheid tot toegang tot elke plaats, in het bijzonder waar het gaat om de activiteiten gerelateerd aan de desbetreffende bijzondere bevoegdheid waartoe de toegang tot de betreffende plaats is vereist, onduidelijkheid en daarmee rechtsonzekerheid te weeg brengt. Ter toelichting hiervan het volgende voorbeeld. Zo is in het huidige artikel 30, eerste lid, aanhef en onder a, de toegang van de dienst tot elke plaats geregeld, voor zover het redelijkerwijs noodzakelijk is om observatie- en registratiemiddelen als bedoeld in artikel 20, eerste lid, onder a, Wiv 2002 aan te brengen. Strikt genomen is de toegang dus beperkt tot het *aanbrengen* van de genoemde middelen. In de praktijk zal echter veelal voorafgaand aan het aanbrengen van dergelijke middelen, een voorverkenning plaatsvinden in bijvoorbeeld de woning om te bezien waar een registratie- of observatiemiddel het beste kan worden aangebracht en of daar extra voorzieningen voor nodig zijn. Vervolgens zal – eventueel op een later moment – overgegaan kunnen worden tot het aanbrengen van een middel. Een middel kan echter gedurende de periode waarbij het wordt ingezet defect geraken en alsdan zal

deze dienen te worden vervangen. Tot slot zal – indien het niet meer noodzakelijk is het middel in te zetten – deze dienen te worden verwijderd (indien dat redelijkerwijs mogelijk is). In het voorgestelde artikel 42 worden thans in relatie tot de bijzondere bevoegdheden waarvoor toegang tot een plaats is vereist de daarmee samenhangende activiteiten omschreven.

De in artikel 42 geregelde bevoegdheid staat niet op zichzelf, maar is ondersteunend aan de inzet van de in het eerste lid aangeduide bevoegdheden. Om die reden is niet voorzien in een (nieuwe) toestemming voor de inzet van deze bevoegdheid (artikel 42, tweede lid). Voor zover het echter gaat om toegang tot woningen geldt echter een aanvullende regeling. Op het binnentreden van woningen door de diensten is de Algemene wet op het binnentreden met uitzondering van een enkele bepaling regulier van toepassing; artikel 42, vierde lid, van het wetsvoorstel geeft ter zake een voorziening. Het binnentreden van woningen door speciaal daarvoor door het hoofd van de dienst aangewezen personen (artikel 42, derde lid) zal in zijn algemeenheid op heimelijke wijze plaatsvinden en derhalve zal in die gevallen geen sprake (kunnen) zijn van toestemming van de bewoner. In dat geval is op grond van artikel 2 van de Algemene wet op het binnentreden een schriftelijke machtiging vereist. In artikel 42, vierde lid, laatste volzin, is de bevoegdheid tot het afgeven van een machtiging in handen gelegd van de voor de desbetreffende dienst verantwoordelijke minister of namens deze het hoofd van de dienst; deze bevoegdheid kan niet worden doorgemandateerd. De machtiging is ingevolge artikel 6, tweede lid, van de Algemene wet op het binnentreden drie dagen geldig vanaf het moment waarop zij is afgegeven. Dat betekent voor de praktijk van de diensten, dat voor de uitoefening van een bijzondere bevoegdheid, waarvoor bijvoorbeeld een toestemming van drie maanden is verleend, daarnaast voor het binnentreden van de woning zonder toestemming van de bewoner het meerdere keren nodig kan zijn om een machtiging als hier bedoeld te verkrijgen; bijvoorbeeld voor het binnentreden ter verkenning van de woning, vervolgens op een later moment voor het plaatsen van technische hulpmiddelen en nog later om deze te verwijderen. Aangezien dit laatste niet altijd mogelijk is binnen de periode waarvoor de toestemming is gegeven voor de uitoefening van de desbetreffende bijzondere bevoegdheid, maar het niettemin noodzakelijk kan zijn om de geplaatste hulmiddelen te verwijderen – om ontdekking daarvan te voorkomen, waardoor anders het onderzoek van de dienst ernstige schade kan oplopen – is in artikel 42, vijfde lid, van het wetsvoorstel voorzien in een specifieke regeling ter zake. Aldaar is het eerste tot en met vierde lid van overeenkomstige toepassing verklaard op het verwijderen van een technisch hulpmiddel, indien de toestemming voor de uitoefening van de bijzondere bevoegdheid in welk kader het technisch hulpmiddel is toegepast inmiddels is beëindigd.

In artikel 42, vierde lid, van het wetsvoorstel zijn voorts de artikelen 1, eerste, tweede en derde lid, alsmede artikel 2, eerste lid, laatste volzin van de Algemene wet op het binnentreden buiten toepassing verklaard. Gelet op het heimelijke karakter van het binnentreden van woningen door daartoe door het hoofd van de dienst aangewezen personen, ligt het niet in de rede bijvoorbeeld een voorafgaande mededeling te doen van het doel van het binnentreden en zich ter zake te legitimeren.

Ingevolge artikel 10 van de Algemene wet op het binnentreden, dient van binnentreden van een woning zonder toestemming van de bewoner een verslag te worden opgesteld. Een afschrift van dit verslag dient vervolgens aan de bewoner te worden uitgebracht. In artikel 10, tweede lid, is vervolgens bepaald wat in een dergelijk verslag dient te staan. Deze bepaling is in artikel 46, vierde lid, van onderhavig wetsvoorstel buiten toepassing verklaard, aangezien in artikel 46, derde lid, ter zake een op de specifieke situatie van de inlichtingen- en veiligheidsdiensten toegespitste regeling wordt gegeven. In artikel 12, derde lid, van de Grondwet is in verband hiermee bepaald, dat indien het binnentreden in het belang van de nationale veiligheid heeft plaatsgevonden, volgens bij de wet te stellen regels de verstrekking van het verslag kan worden uitgesteld. In de bij de wet te bepalen gevallen kan de verstrekking achterwege worden gelaten, indien het belang van de nationale veiligheid zich tegen verstrekking blijvend verzet. In artikel 34 van de Wiv 2002 en in artikel 46 van onderhavig wetsvoorstel is een bijzondere regeling opgenomen voor het uitbrengen van verslag omtrent enkele bijzondere bevoegdheden. Daarin wordt ook het uitbrengen van een verslag als hier bedoeld geregeld, waarbij tevens is voorzien in uitstel- en afstelgronden.

3.3.3.5 Afwegingskader en verslaglegging

In paragraaf 3.2.2.9 van het wetsvoorstel wordt een regeling gegeven voor het bij de uitoefening van bijzondere bevoegdheden toe te passen afwegingskader (de artikelen 43 en 44) alsmede voor de verplichting om van de uitoefening van een bijzondere bevoegdheid een verslag te maken (artikel 45). Deze regeling is ongewijzigd overgenomen uit de huidige wet (artikelen 31, 32 en 33 Wiv 2002).

Bij de uitoefening van enkele van hun onderzoekstaken dan wel ter ondersteuning daarvan in een limitatief aantal gevallen (zie artikel 23 van het wetsvoorstel) zijn de diensten bevoegd tot het uitoefenen van bijzondere bevoegdheden. De zowel in de huidige wet als in onderhavig wetsvoorstel neergelegde bijzondere bevoegdheden zijn verschillend van aard en zijn niet altijd in elke situatie toepasbaar; de omstandigheden van het geval zullen veelal (mede) bepalen welke bijzondere bevoegdheden voor toepassing in aanmerking komen. Als een onderzoekssubject van een dienst geen gebruik maakt van telecommunicatiemiddelen, dan zal de inzet van de bevoegdheid tot

het aftappen van zijn telecommunicatie niet aan de orde zijn. Daartegen kunnen bij het verkrijgen van de voor een onderzoek benodigde gegevens vaak ook door de inzet van meerdere bijzondere bevoegdheden – al dan niet in combinatie met elkaar - worden verkregen. Tussen de verschillende bijzondere bevoegdheden bestaat ook geen absolute rangorde waar het gaat om de vraag – los van de concrete situatie waarin de bevoegdheid zou moeten worden toegepast - welke mate van inbreuk op iemands persoonlijke levenssfeer met de uitoefening van een bepaalde bijzondere bevoegdheid wordt gemaakt. Ter illustratie hiervan: Is video-observatie (statische observatie) zwaarder of lichter dan volgen (dynamische observatie)? Is het aftappen van telecommunicatie zwaarder of lichter dan de toepassing van een microfoon in iemands werkkamer?

Mede gelet op het voorgaande is het dan ook zaak dat de diensten bij de uitoefening van de aan hen toekomende bevoegdheden – toegespitst op de concrete omstandigheden van ieder geval – een nadrukkelijke afweging ter zake maken. Los van de algemeen van toepassing zijnde criteria bij de verwerking van gegevens, zoals neergelegd in de artikelen 17 e.v. van het wetsvoorstel, voorzien de artikelen 43 en 44 in een specifiek toetsingskader dat gehanteerd dient te worden bij de uitoefening van bijzondere bevoegdheden. De in de jurisprudentie ontwikkelde beginselen van proportionaliteit en subsidiariteit kennen hiermee sinds de inwerkingtreding van de Wiv 2002 een wettelijke verankering. In het kader van het door de CTIVD uitgevoerde rechtmatigheidstoezicht op de uitoefening van bijzondere bevoegdheden door de diensten vormen deze beginselen een belangrijke toetssteen.

In artikel 43, eerste lid, is als algemeen uitgangspunt neergelegd, dat de uitoefening van een bijzondere bevoegdheid alleen is geoorloofd, indien de daarmee beoogde verzameling van gegevens niet of niet tijdig kan geschieden door raadpleging van voor een ieder toegankelijke informatiebronnen of van informatiebronnen waarvoor aan de dienst een recht op kennisneming van de aldaar berustende gegevens is verleend. Bij de beantwoording van de vraag of gegevens niet of niet tijdig kunnen worden verzameld, kunnen diverse aspecten een rol spelen. Zo zal in het geval dat er sprake is van een ernstige en acute dreiging, bijvoorbeeld indien er concrete indicaties zijn dat er een aanslag wordt voorbereid, de voor het onderzoek benodigde gegevens zo snel mogelijk dienen te worden verzameld; in een dergelijke situatie zal de beslissing om over te gaan tot de uitoefening van bijzondere bevoegdheden snel gemaakt kunnen worden. Onder niet of niet tijdig kunnen verzamelen van gegevens als bedoeld in dit artikel dient ook de situatie te worden verstaan, waarbij er gerede twijfel bestaat over de volledigheid of de betrouwbaarheid van de gegevens die men wel heeft verkregen door toepassing van de

aldaar genoemde mogelijkheden. Ook in die situatie komt de inzet van bijzondere bevoegdheden in beeld.

Is uiteindelijk besloten tot het verzamelen van gegevens door de uitoefening van een of meer bijzondere bevoegdheden, dan mag slechts die bevoegdheid worden uitgeoefend, die gelet op de omstandigheden van het geval, waaronder de ernst van de bedreiging van de door de dienst te beschermen belangen, mede in vergelijking met andere beschikbare bevoegdheden voor de betrokkene het minste nadeel oplevert (artikel 43, tweede lid). Dit betreft de subsidiariteitstoets. Min of meer in het verlengde daarvan bepaalt artikel 44 dat een bijzondere bevoegdheid onmiddellijk wordt gestaakt, indien het doel waartoe de bevoegdheid is uitgeoefend is bereikt dan wel met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan. De proportionaliteitseis heeft zijn neerslag gekregen in artikel 43, derde en vierde lid: de uitoefening van een bijzondere bevoegdheid dient achterwege te blijven, indien de uitoefening ervan voor betrokkene een onevenredig nadeel in vergelijking met daarmee na te streven doel oplevert; de uitoefening dient evenredig te zijn aan het daarmee beoogde doel.

Een juiste toepassing van het geschetste toetsingsmodel in de dagelijks praktijk van het werk van de inlichtingen- en veiligheidsdiensten is van groot belang om de met de toepassing van de onderscheiden bijzondere bevoegdheden te maken inbreuk op de grondrechten van de burgers, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, te legitimeren en via het vastleggen van de daarbij gemaakte afwegingen deze ook achteraf, zowel in het kader van interne evaluaties als in het kader van het door de CTIVD uit te voeren rechtmatigheidstoezicht, voor toetsing vatbaar te doen zijn. Deze afwegingen zullen over het algemeen onderdeel uitmaken van de verzoeken om toestemming die aan de aangewezen personen en instanties moeten worden overgelegd, zij het dat de aard en mate daarvan van geval tot geval kan verschillen. Waar het om gaat is dat de persoon of instantie die de beslissing moet nemen dit op basis van toereikende gegevens kan verrichten en zich van de gemaakte afwegingen kan vergewissen. In sommige gevallen zal dit kunnen betekenen dat in een verzoek om toestemming wordt volstaan met minder gedetailleerde gegevens dan die welke zich bevinden in een operatiedossier; in dat geval ligt het in de rede dat daarvan ook melding wordt gemaakt, opdat de persoon of instantie die toestemming moet verlenen er alsnog naar kan vragen. Voor het overige geldt dat van de uitoefening van een bijzondere bevoegdheid – voor vergelijkbare redenen als hiervoor gegeven - een schriftelijk verslag wordt gemaakt. Artikel 45 van het wetsvoorstel voorziet daarin.

3.3.3.6 Het uitbrengen van verslag omtrent de uitoefening van enkele bijzondere bevoegdheden

In artikel 34 Wiv 2002 is een regeling opgenomen inzake het uitbrengen van verslag omtrent de uitoefening van enkele – niet alle – bijzondere bevoegdheden die door een dienst jegens personen is ingezet. Deze regeling staat ook wel bekend als de notificatieplicht. Deze regeling is in onderhavig wetsvoorstel in artikel 46 in vrijwel gelijkluidende zin opnieuw opgenomen. Op een enkele aanpassing zal hierna nog nader worden ingegaan. Op de (wets)historische achtergrond voor het opnemen van een notificatieregeling in de Wiv 2002 zal hier niet nader worden ingegaan; kortheidshalve wordt verwezen naar hetgeen daaromtrent in het kader van de parlementaire behandeling van de Wiv 2002 is gewisseld.[71] Voorts is in 2008 door de toenmalige Minister van BZK in een brief aan de Tweede Kamer uitvoerig ingegaan op de diverse *ins and outs* van de notificatieplicht alsmede de daarmee opgedane ervaringen tot dan toe.[72] Daarnaast heeft de CTIVD in 2010 een rapport uitgebracht naar aanleiding van haar onderzoek inzake de rechtmatigheid van de uitvoering van de notificatieplicht door de AIVD[73]; een vergelijkbaar onderzoek met betrekking tot de MIVD heeft tot op heden overigens niet plaatsgevonden. Hoewel in de afgelopen jaren de vraag naar nut en noodzaak van een notificatieregeling enkele malen aan de orde is gesteld, ook door de CTIVD in het hiervoor genoemde rapport, zij het met de kanttekening dat deze afweging door de wetgever dient te worden gemaakt, wordt de notificatieplicht in onderhavig wetsvoorstel gehandhaafd. De constatering van de CTIVD in haar rapport uit 2010 dat de tenuitvoerlegging van de notificatieplicht een aanzienlijk beslag legt op de capaciteit van de AIVD en dat dit in de toekomst zeer waarschijnlijk alleen maar zal toenemen, is juist; evenals de bevinding dat uit het EVRM en de relevante rechtspraak niet expliciet een actieve notificatieplicht kan worden afgeleid en dat het gewicht van zo'n plicht moet worden afgezet tegen het geheel van overigens aanwezige rechtswaarborgen.[74] Dit laatste is ook van meet af aan het standpunt geweest van de regering in het kader van de voorbereiding van de huidige wet. Wel is het anderszins zo, dat niet zozeer uit het EVRM maar wel uit artikel 12 Grondwet een verslagverplichting voortvloeit, waar het gaat om het binnentreden in een woning zonder toestemming van de bewoner; zie artikel 12, derde lid, Grondwet.[75] Bij de bespreking van artikel 42 is daar reeds bij stilgestaan. Een volledige afschaffing van de notificatieplicht – zo die al zou worden overwogen - is gelet daarop dan ook niet mogelijk.

In artikel 46, eerste lid, is de onderzoeksverplichting voor de minister geformuleerd om vijf jaar na beëindiging van de uitoefening van een bijzondere bevoegdheid als bedoeld in

[71] Kamerstukken II 1999/2000, 25 877, nr. 8, blz. 87-88.
[72] Kamerstukken II 2008/09, 30 977, nr. 18.
[73] CTIVD-rapport nr. 24 (2010).
[74] CTIVD-rapport nr. 24 (2010), blz. 27.
[75] Inwerkingtreding per 21 maart 2002 (Stb. 2002, 144).

de artikelen 29, eerste lid (openen van brieven en andere geadresseerde zendingen), artikel 30, tweede lid, onder c (aanbrengen van technische voorzieningen met het oog op de toepassing van artikel 25, eerste lid, en 32, eerste lid), voor zover toegepast in een woning zonder toestemming van de bewoner, 32, eerste lid (gericht afluisteren), alsmede artikel 42, eerste lid, voor zover is binnengetreden in een woning zonder toestemming van de bewoner, en daarna telkens eenmaal per jaar, te onderzoeken of de persoon ten aanzien van wie één van deze bijzondere bevoegdheden is uitgeoefend, daarvan verslag kan worden uitgebracht. In artikel 46, derde lid, is vervolgens bepaald wat de inhoud van dit verslag dient te zijn.

Zoals hiervoor reeds is aangegeven is de reikwijdte van de onderzoeksverplichting aangepast. Enerzijds is een bijzondere bevoegdheid toegevoegd ten aanzien waarvan voortaan ook onderzocht dient te worden of ter zake van de uitoefening daarvan verslag kan worden uitgebracht; het betreft hier de bijzondere bevoegdheid, waarbij in het kader van de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk technische voorzieningen worden aangebracht in verband met de toepassing van de bevoegdheid als bedoeld in de artikelen 25, eerste lid, en 32, eerste lid, van het wetsvoorstel in een woning zonder toestemming van een bewoner (artikel 30, eerste lid, aanhef en onder b jo. tweede lid, onder c). Weliswaar wordt dan niet fysiek de woning betreden, maar de inbreuk op iemands persoonlijke levenssfeer door uitoefening van de desbetreffende bevoegdheid is wel vergelijkbaar met de situatie waarbij de woning wel is betreden en waarbij geluids- of videoapparatuur is geplaatst. In laatstgenoemde situatie dient vanwege de inbreuk op het huisrecht wel genotificeerd te worden. Hoewel niet helemaal met elkaar vergelijkbaar, wordt het niettemin wenselijk geacht ook hier tot notificatie over te gaan. Anderzijds komt de onderzoeksverplichting die nu bestaat met betrekking tot de toepassing van de bevoegdheid tot selectie als bedoeld in artikel 27, derde lid, onder a (op gegevens betreffende de identiteit van een persoon dan wel organisatie) en b (op een nummer dan wel technisch kenmerk), Wiv 2002 te vervallen. Met de introductie van het nieuwe interceptiestelsel wordt in fase 3, welke in artikel 35 nader is uitgewerkt, namelijk voorzien in een ander stelsel voor de selectie van gegevens in de bulk aan gegevens die op grond van artikel 33, eerste lid, is verworven. Daarbij wordt aangesloten bij de systematiek die thans ook reeds geldt voor selectie op trefwoorden gerelateerd aan door de minister geaccordeerde onderwerpen (artikel 27, derde lid, jo. vijfde lid, Wiv 2002); daarbij wordt geen onderscheid meer gemaakt in de soort selectiecriteria. In het nieuwe stelsel is er geen sprake meer van de uitoefening van een bevoegdheid tot selectie jegens bijvoorbeeld een persoon of organisatie, maar is deze bevoegdheid gekoppeld aan een door de minister ter zake geaccordeerd onderzoek; het vaststellen van selectiecriteria, ook indien dit namen of nummers betreft, is voortaan

een uitvoeringshandeling en niet meer een zelfstandige bevoegdheid waarvoor op de voet van artikel 24 van het wetsvoorstel toestemming is vereist. Er liggen dan ook geen "sigint-lasten" meer voor met betrekking personen of organisaties dan wel gerelateerd aan nummers of technisch kenmerken, zoals thans nog het geval is. Overigens kan voor de huidige situatie worden opgemerkt dat tot op heden door de diensten nimmer een verslag is uitgebracht waar het gaat om de toepassing van de huidige selectiebevoegdheid met betrekking tot personen, organisaties of nummers (artikel 27, derde lid, onder a en b, Wiv 2002). Of de betrokkenen zijn niet te traceren, dan wel vindt afstel van notificatie plaats vanwege het feit dat dit tot ernstige schade aan de betrekkingen met andere landen en internationale organisaties kan leiden (artikel 34, zevende lid, aanhef en onder b, Wiv 2002).

Met de termijn van vijf jaar is aangesloten bij de termijn van vijf jaar die in artikel 70, eerste lid, onder a, sub 1, van het wetsvoorstel is opgenomen (huidig artikel 63 Wiv 2002) waar de weigeringsgrond die betrekking heeft op het "actuele kennisniveau" van de dienst is uitgewerkt; daarbij wordt ervan uitgegaan dat gegevens die minder dan vijf jaar geleden zijn verwerkt zicht geven op het actueel kennisniveau van de dienst. Nu een verzoek om inzage in dergelijke gegevens op grond van artikel 70 van het wetsvoorstel dient te worden geweigerd, ligt het niet voor de hand om dan wel een verslag van een uitgeoefende bevoegdheid jegens betrokkene uit te brengen indien die vijfjarentermijn nog niet is verstreken. Temeer nu notificatie aan betrokkene kan leiden tot een inzageverzoek, die vervolgens vanwege die vijfjarentermijn zonder meer moet worden geweigerd. Zowel vanwege de inhoudelijke samenhang tussen inzage en notificatie als vanuit een oogpunt van wetsystematiek ligt aansluiting bij de vijfjarentermijn in artikel 70 dan ook voor de hand.[76]

De onderzoeksverplichting geldt voor elk van de genoemde bijzondere bevoegdheden, zodra de inzet daarvan jegens de desbetreffende persoon is beëindigd. Het gaat dan om het moment waarop de termijn waarvoor toestemming is verleend – inclusief eventuele ononderbroken verlengingen – afloopt. In de praktijk zal het veelal zo zijn dat in geval verschillende bijzondere bevoegdheden ten aanzien van een persoon zijn uitgeoefend, al deze bevoegdheden binnen het kader van een bepaald onderzoek waarin de betreffende persoon is betrokken zijn toegepast; dat zal dan ook met zich meebrengen dat in feite het onderzoek naar de laatst uitgeoefende – en voor notificatie in aanmerking komende - bijzondere bevoegdheid (mede) bepalend is voor het antwoord op de vraag of ook ten aanzien van andere, eerder uitgeoefende – en voor notificatie in aanmerking komende - bijzondere bevoegdheden tot het uitbrengen van een verslag kan worden overgegaan.

[76] Zie ook Kamerstukken II 1999/2000, 25 877, nr. 8, blz. 90.

Notificatie ten aanzien van eerder uitgeoefende bevoegdheden kan immers leiden tot schade aan een lopend onderzoek en geeft voorts zicht op het actueel kennisniveau van de dienst. In die situatie zal voor die eerder uitgeoefende bevoegdheden dan ook een uitstelgrond van toepassing zijn. Dit ligt echter anders indien er sprake is van uitoefening van bijzondere bevoegdheden jegens een persoon in het kader van verschillende onderzoeken zonder dat daarbij sprake is van onderlinge samenhang.[77]

De notificatieverplichting bestaat uitsluitend jegens de natuurlijke personen *ten aanzien van wie* de desbetreffende bijzondere bevoegdheid is uitgeoefend. Er bestaat geen notificatieplicht jegens organisaties, hoewel daartegen als zodanig eveneens bijzondere bevoegdheden kunnen worden ingezet. Evenals de CTIVD in haar eerder genoemde rapport (nr. 24) met betrekking tot de AIVD heeft uiteengezet, geldt de notificatieplicht ingeval bijzondere bevoegdheden zijn ingezet tegen (1) 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 (zogeheten a-taak van de AIVD; deze personen worden aangeduid als *targets*), (2) personen die niet als een target worden aangemerkt, maar waarbij de inzet van de bijzondere bevoegdheid ertoe kan leiden dat de informatiepositie ten aanzien van een target wordt verbeterd (*non-targets*) en (3) personen die in het kader van de uitoefening van de zogeheten buitenlandtaak (onderzoek naar andere landen) worden onderzocht. Waar het gaat om de uitoefening van bijzondere bevoegdheden jegens organisaties merkt de CTIVD terecht op dat daarbij ook vaak inbreuk wordt gemaakt op de persoonlijke levenssfeer van personen. Onder omstandigheden geldt dan ook in die gevallen een notificatieplicht, namelijk indien de uitoefening van de bijzondere bevoegdheid (tevens) gericht is op specifieke individuele leden van de organisatie; daarbij is indifferent of de afgeluisterde communicatie in de werk- of in de privésfeer plaatsvond.[78] Het voorgaande geldt *mutatis mutandis* voor de MIVD.

De onderzoeksverplichting ontstaat, zoals eerder aangegeven, vijf jaar na beëindiging van de uitoefening van de desbetreffende bijzonder bevoegdheid. Bij de beoordeling van de vraag of tot het uitbrengen van een verslag kan worden overgegaan, dient acht te worden geslagen op de toepasselijke uitstel- en afstelgronden; artikel 46, zesde, onderscheidenlijk zevende lid, voorzien daarin. Bij de regeling inzake de uitstelgronden is aansluiting gezocht bij de regeling inzake de kennisneming van persoonsgegevens. Het uitbrengen van een verslag dient te worden uitgesteld, indien de desbetreffende bijzondere bevoegdheid is uitgeoefend in het kader van een onderzoek, waaromtrent

[77] Zie ook Kamerstukken II 2000/2001, 25 877, nr. 14, blz. 57.
[78] Zie CTIVD-rapport nr. 24, blz. 7 en 8.

versrekking van gegevens aan de betrokken persoon, indien deze op het moment van onderzoek een aanvraag als bedoeld in artikel 64 zou hebben ingediend, ingevolge artikel 70 zou moeten worden geweigerd. In het geval het uitbrengen van een verslag dient te worden uitgesteld, herleeft na een jaar de onderzoeksverplichting (artikel 46, eerste lid). Het is echter mogelijk dat uit het onderzoek blijkt dat er sprake is van een afstelgrond als bedoeld in artikel 46, zevende lid, als gevolg waarvan de verplichting tot onderzoek op grond van het eerste lid komt te vervallen. Daarvan kan sprake zijn, indien het uitbrengen van een verslag naar redelijke verwachting ertoe leidt dat (a) bronnen van een dienst, daaronder begrepen inlichtingen- en veiligheidsdiensten van andere landen, worden onthuld; (b) betrekkingen met andere landen en met international organisatie ernstig worden geschaad; en (c) een specifieke toepassing van een methode van een dienst of de identiteit van degene die de betrokken dienst behulpzaam is geweest bij de toepassing van de methode wordt onthuld. Bij de parlementaire behandeling van de Wiv 2002 is opgemerkt dat er twee momenten zijn, waarbij kan worden vastgesteld of een afstelgrond aan de orde is, namelijk (a) bij gelegenheid van de uitoefening van de desbetreffende bijzondere bevoegdheid, waardoor nimmer een onderzoek hoeft te worden verricht, dan wel (b) bij gelegenheid van het onderzoek of tot notificatie kan worden overgegaan. Daarbij werd opgemerkt dat de gronden van afstel immers van dien aard zijn dat indien eenmaal is vastgesteld dat daaraan wordt voldaan deze vervolgens ook blijven gelden.[79] Hoewel uit de wetsgeschiedenis derhalve blijkt dat de mogelijkheid aanwezig is om reeds bij de uitoefening van een bijzondere bevoegdheid te bezien of een afstelgrond van toepassing is (hetgeen vanuit overwegingen van efficiëntie aangewezen kan zijn), wordt in dergelijke gevallen op het moment dat de onderzoeksplicht ontstaat (na vijf jaar) opnieuw getoetst of de eerder (in indicatieve zin) vastgestelde afstelgrond inderdaad (nog) aanwezig is.[80] Dat kan met name van belang zijn ingeval een beroep is gedaan op de afstelgrond dat door het uitbrengen van een verslag een specifieke toepassing van een methode van een dienst zou worden onthuld; een beroep daarop is alleen aan de orde indien het gaat om een methode die (nog) niet algemeen bekend is, zoals bijvoorbeeld bij nieuwe technische hulpmiddelen of nieuwe toepassingen van bestaande technische hulpmiddelen die nog niet algemeen bekend (kunnen) zijn. Dit zal alsdan van geval tot geval dienen te worden beoordeeld. Bij die afweging is overigens ook van belang dat in het uit te brengen verslag, slechts dient te worden volstaan met een aanduiding van de bijzondere bevoegdheid als bedoeld in artikel 46, eerste lid, die ten aanzien van de betrokken persoon is uitgeoefend (artikel 46, derde lid, onder b).

[79] Zie Kamerstukken II 1999/2000, 25 877, nr. 8, blz. 91.
[80] Kamerstukken II 2008/09, 30 977, nr. 18, blz. 5.

Naast de hiervoor besproken uitstel- en afstelgronden voorziet het wetsvoorstel, evenals de huidige wettelijke regeling, in een vervalgrond. In artikel 46, vijfde lid, is namelijk bepaald dat de verplichting tot het uitbrengen van een verslag vervalt op het moment dat is vastgesteld dat zulks redelijkerwijs niet mogelijk is. Daarvan is concreet sprake, indien de persoon waaraan het verslag zou moeten worden uitgebracht niet te traceren valt, dan wel is gebleken dat deze is overleden. Zoals door de Minister van BZK in reactie op het eerder genoemde rapport van de CTIVD is aangegeven, wordt bij het traceren van betrokkene niet alleen de GBA (thans basisregistratie personen) geraadpleegd en aanvullend een zoekslag in de eigen informatiesystemen van de dienst, maar zal bij de zoekslag in de eigen informatiesystemen ook zelfstandig worden bezien op aanwijzingen omtrent de verblijfplaats van de betrokkene. En indien er op basis van de voorhanden zijnde gegevens indicaties zijn omtrent de verblijfplaats van de betrokkene, zal bij een RID dan wel een andere relevante bron, worden nagevraagd of deze informatie beschikt over informatie omtrent de verblijfplaats van de betrokkene.[81]

Indien het onderzoek als bedoeld in artikel 46, eerste lid, (op enig moment) leidt tot de conclusie dat een verslag kan worden uitgebracht, dan dient dit zo spoedig mogelijk te gebeuren. Het onderzoek kan er echter ook toe leiden dat – om verschillende redenen (zie hiervoor) – wordt geconcludeerd dat dit niet mogelijk is. In dat geval dient op grond van artikel 46, tweede lid, van het wetsvoorstel de CTIVD daarvan met redenen omkleed op de hoogte te worden gesteld.

3.3.4 Bijzondere bepalingen inzake geautomatiseerde data-analyse

De diensten zijn op grond van artikel 17, eerste lid, van het wetsvoorstel bevoegd tot het verwerken van gegevens (persoonsgegevens en andere gegevens). Aan deze verwerking zijn diverse eisen gesteld, zoals in paragraaf 3.2 van deze toelichting reeds uiteen is gezet. De verwerking vindt slechts plaats voor een bepaald doel en indien dit noodzakelijk is voor een goede taakuitvoering. Bovendien dient de verwerking te geschieden in overeenstemming met de wet en op zorgvuldige wijze. Het begrip "verwerken" is in artikel 1 van het wetsvoorstel gedefinieerd en omvat – kort gezegd – elke handeling of elk geheel van handelingen met betrekking tot gegevens, daaronder ook begrepen het vergelijken en het met elkaar in verband brengen van gegevens. Dit zijn voorbeelden van "data-analyse".

Geautomatiseerde data-analyse is een verwerkingsmethode die brede ingang heeft gevonden in alle sectoren van de samenleving; overheid, bedrijven en particulieren maken daarvan gebruik om de toenemende hoeveelheid van beschikbare gegevens op

[81] Kamerstukken II 2009/10, 29 924, nr. 49.

een effectieve en efficiënte wijze te kunnen verwerken. Bovendien leidt het ontstaan van "big data", te weten het fenomeen dat de hoeveelheid data exponentieel groeit, dataverzamelingen steeds groter en complexer worden en relevante data als gevolg daarvan niet meer fysiek of logisch in een locatie of in een systeem kunnen worden opgeslagen, ertoe dat deze nog uitsluitend met toepassing van geavanceerde vormen van data-analyse op een effectieve en efficiënte manier is te benaderen.

Ook inlichtingen- en veiligheidsdiensten passen sinds jaar en dag diverse vormen van geautomatiseerde data-analyse toe. Echter, meer dan wellicht in andere overheidssectoren het geval is, brengt de aard van de werkzaamheden van deze diensten met zich dat zich hier de spanning tussen veiligheid en privacy zich het meest indringend – in ieder geval in de beleving van veel mensen – doet voelen. In de afgelopen jaren is over de thematiek privacy en veiligheid reeds veel geschreven en gesproken, ook juist in relatie tot de werkzaamheden van inlichtingen- en veiligheidsdiensten. Daarbij is van overheidswege telkens benadrukt dat het bij (nationale) veiligheid en privacy niet om tegengestelde belangen gaat, maar dat deze veeleer in elkaars verlengde liggen.

Zoals eerder is betoogd, is gegevensverwerking de kernactiviteit van inlichtingen- en veiligheidsdiensten. In onderhavig wetsvoorstel wordt deze kernactiviteit – met inachtneming van de eisen die daaraan vanuit grond- en mensenrechtelijk perspectief zijn te stellen – in al zijn onderdelen duidelijk genormeerd en van toereikende waarborgen voorzien. Mede gelet hierop is het ook wenselijk om geautomatiseerde data-analyse als werkmethode van de diensten van een expliciete wettelijke grondslag te voorzien. Het voorgestelde artikel 47 strekt daartoe. Voorts wordt daarmee – in combinatie met hetgeen is bepaald in artikel 35, eerste lid, onder b, van het wetsvoorstel – een regeling gegeven voor de eerder – in het kader van het onderzoek van communicatie – besproken metadata-analyse.

In artikel 47, eerste lid, wordt geëxpliciteerd dat de diensten bevoegd zijn om geautomatiseerde data-analyse uit te voeren met betrekking tot gegevens uit eigen geautomatiseerde gegevensbestanden, gegevens uit voor een ieder toegankelijke informatiebronnen, gegevens uit geautomatiseerde gegevensbestanden waartoe de diensten rechtstreeks toegang hebben en gegevens uit daartoe door derden verstrekte (delen van) geautomatiseerde gegevensbestanden.

Voor alle vormen van data-analyse geldt echter onverkort dat deze slechts toegepast mogen worden in het kader van een goede taakuitvoering van de diensten; dat vloeit voort uit artikel 17 van het wetsvoorstel. Zoals uit artikel 47, eerste lid, blijkt kunnen bij data-analyse ook gegevens uit door derden ter beschikking gestelde gegevensbestanden

worden gebruikt. Daarin zitten onvermijdelijk ook gegevens van personen die niet de aandacht van de diensten hebben, maar waarvan de verwerking van die gegevens - omdat deze nu eenmaal een logisch en onlosmakelijk onderdeel uitmaken van een dergelijk gegevensbestand - niettemin noodzakelijk is om de data-analyse te kunnen uitvoeren. Aangezien de wet duidelijkheid dient te geven omtrent wie door de diensten gegevens kunnen worden verwerkt, is in artikel 18, vijfde lid, van het wetsvoorstel daartoe een regeling opgenomen.

In artikel 47, tweede lid, is aangegeven welke vormen van data-analyse in ieder geval onder de in het eerste lid geëxpliciteerde bevoegdheid kunnen worden begrepen. Deze opsomming is niet limitatief, immers de toepassing van eventuele nieuwe methoden en technieken moet mogelijk zijn. In het tweede lid worden echter drie veel voorkomende vormen van data-analyse benoemd: (a) het op geautomatiseerde wijze onderling vergelijken, dan wel in combinatie met elkaar vergelijken van gegevens, (b) het doorzoeken van gegevens aan de hand van profielen en (c) het vergelijken van gegevens met het oog op het opsporen van bepaalde patronen.

In artikel 47, derde lid, is ten slotte bepaald dat het bevorderen of treffen van maatregelen jegens een persoon uitsluitend op basis van de resultaten van een gegevensverwerking als bedoeld in het tweede lid , aanhef en onder b, niet is toegestaan. Het gaat hier om het doorzoeken van gegevens op basis van een profiel. Een dergelijk profiel behelst veelal 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. Dit is echter geen statisch, maar dynamisch proces waarbij aan de hand van nieuwe inzichten en gegevens tot bijstelling van het profiel kan worden gekomen. Op grond van de voorgestelde regeling is het de diensten niet toegestaan om louter op basis van de toepassing van een dergelijk profiel gegenereerde resultaten jegens de desbetreffende persoon maatregelen te treffen of te bevorderen. Er dient met andere woorden ook nog een menselijke afweging ter zake worden gemaakt.

3.3.5 De verstrekking van gegevens

3.3.5.1 Algemeen

In paragraaf 3.4 van het wetsvoorstel wordt een regeling gegeven voor de verstrekking van gegevens. Deze regeling komt vrijwel geheel overeen met de bestaande regeling in paragraaf 3.3 van de Wiv 2002. Op drie onderdelen is zij echter aangepast. Allereerst is in artikel 49 van het wetsvoorstel een ten opzichte van het huidige artikel 36 Wiv 2002

aanvullende bepaling opgenomen waar het gaat om de verstrekking van ongeëvalueerde gegevens. Ten tweede wordt in artikel 50 van het wetsvoorstel een regeling opgenomen voor de verstrekking van gegevens in het kader van de zogeheten 'naslag'; het betreft een nieuw voorschrift dat samenhangt met de in artikel 8, tweede lid, onder f, onderscheidenlijk 10, tweede lid, onder g, van het wetsvoorstel aan de AIVD onderscheidenlijk MIVD opgedragen nieuwe taak. Een derde aanpassing betreft het schrappen van de aangifteplicht in de regeling die voorziet in het doen van mededelingen aan het openbaar ministerie van gegevens die tevens van belang kunnen zijn voor de opsporing of vervolging van strafbare feiten.

Evenals thans het geval is, kent het wetsvoorstel een gesloten verstrekkingstelsel. Dat wil zeggen dat verstrekking van gegevens door de diensten alleen mogelijk is, indien onderhavige wet daarin voorziet (zie artikel 49, vierde lid). Dit is wenselijk gelet op het bijzondere karakter van de gegevens die door of ten behoeve van de diensten worden verwerkt. Zo geeft het wetsvoorstel een regeling van de gegevensverstrekking in het kader van de taakuitvoering van de diensten (met daarbij de mogelijkheid om onder voorwaarden ook zogeheten 'bijvangst' aan personen en instanties te verstrekken; zie de artikelen 52 en 53 (de huidige artikelen 38 en 39 Wiv 2002)), de verstrekking van gegevens naar aanleiding van verzoeken om kennisneming daarvan (zie hoofdstuk 5 van het wetsvoorstel), en de verstrekking van gegevens in het kader van de samenwerking tussen de beide diensten en met collega-diensten van andere landen (artikelen 74 en 77 van het wetsvoorstel). Op de verstrekking van gegevens zijn uiteraard de bepalingen die betrekking hebben op de verwerking van gegevens in zijn algemeenheid van toepassing.

3.3.5.2 De interne verstrekking van gegevens

In de regeling inzake verstrekking van gegevens, wordt onderscheid gemaakt tussen de interne verstrekking van gegevens en de externe verstrekking van gegevens. In artikel 48 van het wetsvoorstel (huidig artikel 35) wordt voor de interne verstrekking een regeling gegeven. Onder interne verstrekking wordt verstaan de verstrekking aan een binnen de dienst werkzame ambtenaar; voorts wordt daartoe gerekend de verstrekking van gegevens aan de ambtenaren, bedoeld in de artikelen 79 onderscheidenlijk 80, voor zover zij – binnen het kader van genoemde artikelen – werkzaamheden verrichten voor de AIVD onderscheidenlijk de MIVD. Ingevolge artikel 48 van het wetsvoorstel vindt verstrekking van door of ten behoeve van een dienst verwerkte gegevens slechts plaats, voor zover dat noodzakelijk is voor een goede taakuitvoering van de aan de desbetreffende ambtenaar opgedragen taak. Hiermee wordt het zogeheten "need to know"-beginsel tot uitdrukking gebracht. Gelet op het bijzondere karakter van de gegevens, waarbij vaak de persoonlijke levenssfeer in het geding is, dient de

verspreiding van dergelijke gegevens beperkt te blijven tot die medewerkers die daar gelet op de aan hen opgedragen taak kennis van moeten nemen.

3.3.5.3 De externe verstrekking van gegevens

In paragraaf 3.4.2 wordt de externe verstrekking van gegevens geregeld. Het gaat daarbij om de verstrekking van gegevens aan personen en instanties buiten de AIVD en MIVD. Het verrichten van onderzoek door de AIVD en MIVD heeft immers in de kern tot doel de verantwoordelijke instanties tijdig te kunnen waarschuwen voor mogelijke bedreigingen van de in hun respectieve taakomschrijving genoemde gewichtige belangen, dan wel te informeren omtrent gegevens die van belang kunnen zijn voor het te voeren buitenlandbeleid van de regering. Deze verstrekking kan verschillende verschijningsvormen aannemen. De meest bekende is die van het ambtsbericht[82]; maar ook kan het bijvoorbeeld gaan om ten behoeve van zogeheten belangendragers opgestelde specifieke analyses gaan.[83] Naast de algemene bepalingen die op de externe verstrekking van gegevens zien, worden ook nog enkele bijzondere bepalingen gegeven waar het gaat om de externe verstrekking van persoonsgegevens (artikelen 54 tot en met 56). De verstrekking van persoonsgegevens dient met extra waarborgen te worden omgeven, temeer nu de instanties waaraan deze gegevens worden verstrekt veelal ook bevoegd zijn jegens de persoon waarop de gegevens betrekking hebben maatregelen te treffen. Overigens kan onder omstandigheden ook in andere gevallen de verstrekking van (andere) gegevens ertoe leiden dat er jegens bijvoorbeeld een rechtspersoon maatregelen worden getroffen. Het is evident dat dan ook zorgvuldig dient te worden gehandeld; dit vloeit in algemene zin voort uit artikel 17 van het wetsvoorstel.

3.3.5.3.1 Algemene bepalingen

Artikel 49: verstrekking in het kader van een goede taakuitvoering van de diensten

In artikel 49 wordt een (algemene) regeling gegeven voor de verstrekking van gegevens door de diensten *in het kader van een goede taakuitvoering*. Afgezien van het bepaalde in artikel 49, derde lid, is de opgenomen verstrekkingsregeling identiek aan hetgeen

[82] Over het algemeen zal het ambtsbericht een "open" karakter hebben, waarmee wordt bedoeld dat deze zodanig is opgesteld dat van de inhoud daarvan zonder bezwaar kennis kan worden genomen door de betrokken persoon waarop het ambtsbericht betrekking heeft. Er zijn echter ook ambtsberichten die vanwege de inhoud gerubriceerd zijn en waarvan dus door de betrokken persoon geen kennis genomen mag worden; een voorbeeld hiervan vormen de mededelingen die de AIVD doet aan het Ministerie van Buitenlandse Zaken inzake aanvragen voor bepaalde exportvergunningen (zoals *dual use*-goederen).

[83] Deze dienen te worden onderscheiden van openbare – voor het brede publiek bestemde - publicaties van de diensten die ingaan op verschillende fenomenen. Vergelijk de publicaties van de AIVD inzake transformatie van het jihadisme in Nederland (30 juni 2014), Links activisme en extremisme, divers en diffuus, wisselvallig en wispelturig (2 september 2013) en Het jihadistisch internet: kraamkamer van de hedendaagse jihad (14 februari 2012). Zie ook www.aivd.nl.

thans in artikel 36 Wiv 2002 is geregeld. De bevoegdheid tot het verstrekken van gegevens is daarbij in algemene zin in handen gelegd bij de diensten, zij het dat er situaties kunnen voordoen waarbij de verstrekking gelet de aard van de mededeling dient plaats te vinden door de voor de dienst verantwoordelijke minister (zie artikel 49, tweede lid). Dit zal met name dan aan de orde zijn, wanneer er bijvoorbeeld grote politieke risico's aan de verstrekking van de desbetreffende gegevens zijn verbonden.

Evenals nu wordt in artikel 49 gesproken over het doen van een *mededeling* omtrent door of ten behoeve van de dienst verwerkte gegevens. Hetgeen daaromtrent bij de parlementaire behandeling van de huidige wet is gesteld, is nog steeds ter zake doend.[84] Hoewel de mededeling als zodanig ook als een verstrekking van gegevens door de dienst moet worden aangemerkt, is met name voor dit begrip gekozen om tot uitdrukking te brengen dat het veelal zal gaan om op enigerlei wijze door de diensten bewerkte gegevens en niet om de (oorspronkelijke) aan de mededeling ten grondslag liggende gegevens. Het verstrekken van oorspronkelijke gegevens zal overigens vaak ook niet mogelijk zijn, omdat daarmee mogelijk bronnen en *modus operandi* van de diensten worden prijsgegeven. Ingevolge artikel 20 van het wetsvoorstel dienen de hoofden zorg te dragen voor de geheimhouding van daarvoor in aanmerking komende bronnen en *modus operandi*; deze algemene aan de gegevensverwerking gestelde norm, moet ook bij de verstrekking van gegevens in acht genomen worden. In de gevallen waar het echter noodzakelijk wordt geacht om, gelet op de aard van de mededeling en de gevolgen die daaraan kunnen worden verbonden, op voorwaarde van geheimhouding ook inzage te kunnen verlenen in de aan een mededeling ten grondslag liggende (oorspronkelijke) gegevens wordt daarvoor in het wetsvoorstel een aparte voorziening getroffen; zie bijvoorbeeld artikel 52, derde lid, 53, tweede lid, 54, derde lid en 55, vierde lid, van het wetsvoorstel. Waar het gaat om mededelingen aan het openbaar ministerie (artikel 52) dient de inzage desgevraagd te worden verleend; in de andere gevallen bestaat ter zake een discretionaire bevoegdheid.

In artikel 49, eerste lid, zijn evenals thans het geval is een viertal categorieën van instanties benoemd aan wie in het kader van een goede taakuitvoering van de diensten mededelingen kunnen worden gedaan. Het gaat hier om (1) de ministers, (2) andere bestuursorganen en (3) andere personen of instanties, voor zover de mededeling hen aangaat. Daarnaast kan de verstrekking ook plaatsvinden aan (4) daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen, alsmede andere daarvoor in aanmerking komende internationale beveiligings-, verbindinginlichtingen- en inlichtingenorganen.

[84] Zie Kamerstukken II 1997/98, 25 877, nr. 3, blz. 56.

Met de toevoeging "wie deze aangaan" bij de eerste drie categorieën van instanties wordt beoogd tot uitdrukking te brengen, dat de geadresseerde van de mededeling een bijzondere betrokkenheid dient te hebben bij de problematiek waarop de mededeling betrekking heeft. Het criterium "wie deze aangaan" bepaalt dan ook mede de geslotenheid van het verstrekkingensysteem.

In artikel 49, derde lid, is thans een regeling opgenomen voor de verstrekking van ongeëvalueerde gegevens, hetgeen veelal grote hoeveelheden (bulk) betreft, aan buitenlandse collega-diensten. De verstrekking van dergelijke gegevens mag slechts plaatsvinden na toestemming van de voor de dienst verantwoordelijke minister. Uit het gebruik van de term "ongeëvalueerd" blijkt reeds dat het hier niet om een mededeling zal gaan, zoals eerder is toegelicht en vormt daarop dan ook een uitzondering. De opneming van een dergelijke regeling was reeds aangekondigd in de kabinetsreactie op het rapport van de commissie Dessens van 11 maart 2014.[85] Hoewel de aanleiding voor het opnemen van deze regeling primair ligt in de uitwisseling met buitenlandse collega-diensten van grote hoeveelheden metadata, die in het kader van de uitoefening van de bijzondere bevoegdheid tot ongerichte interceptie ex artikel 27 Wiv 2002 (artikel 33 van het wetsvoorstel) worden vergaard, is de in artikel 49 opgenomen regeling breder van opzet en ziet zij op *alle* soorten van gegevens. Daarbij is er tevens voor gekozen deze te doen uitstrekken tot alle ongeëvalueerde gegevens en dus niet te beperken tot de gevallen dat het daarbij gaat om grote hoeveelheden. Het laat zich immers lastig vast stellen wat een grote hoeveelheid is. Bepalend element is dat het gaat om gegevens, waarvan de relevantie voor de eigen taakuitvoering (nog) niet is vastgesteld.

Zoals in paragraaf 2.2 van deze toelichting is aangegeven wordt de taakstelling van beide diensten aangevuld met de taak om op een daartoe strekkend verzoek van een bij regeling van de Minister-president, Minister van Algemene Zaken, en de Ministers van BZK en van Defensie gezamenlijk aangewezen persoon of instantie doen van mededeling omtrent door de dienst verwerkte gegevens omtrent personen of instanties in bij die regeling aangewezen gevallen; het betreft hier een codificatie van een bestaande praktijk, te weten het verrichten van naslagen. In artikel 50 van het wetsvoorstel wordt een nadere regeling gegeven voor de verstrekking van gegevens in dit kader alsmede voor het daaraan ten grondslag liggende verzoek. Deze regeling ziet op een specifieke categorie van verstrekkingen die plaatsvindt in het kader van een goede taakuitvoering van de diensten. In artikel 50, eerste lid, is bepaald dat op een daartoe strekkend schriftelijk verzoek als bedoeld in artikel 8, tweede lid, onder f, en artikel 10, tweede lid, onder g mededeling kan worden gedaan omtrent door de dienst verwerkte gegevens

[85] Kamerstukken II 2013/14, 33 820, nr. 2, blz. 7.

omtrent een persoon of instantie. Een dergelijk verzoek constitueert niet een verplichting om een dergelijke mededeling te doen; of aan een dergelijk verzoek wordt voldaan staat ter discretie van de verantwoordelijk minister, zij het dat in een aantal gevallen, zoals ingeval van kandidaat-bewindslieden, dergelijke verzoeken altijd worden gehonoreerd. In artikel 50, tweede lid, is bepaald aan welke eisen een verzoek als bedoeld in het eerste lid, ten minste dient te voldoen. Het verzoek dient te worden gericht aan – afhankelijk van de dienst die de naslag zou moeten verrichten – de Minister van BZK of de Minister van Defensie. In het verzoek moeten de naam, voornamen, adres en geboortedatum van de betrokken persoon dan wel identificerende gegevens betreffende de instantie te worden opgenomen. Uitgangspunt is daarnaast dat degene naar wie een naslag wordt verricht instemt met het verzoek en dat ter zake een verklaring wordt overgelegd. Deze eis brengt met zich mee dat ten opzichte van de huidige situatie, waarbij in bepaalde gevallen er nog van wordt uitgegaan dat betrokkene impliciet met de naslag heeft ingestemd[86], voortaan een schriftelijke verklaring dient te worden overgelegd. Weliswaar leidt dit tot extra administratieve lasten, maar daartegenover staat dat betrokkene nader kan worden geïnformeerd over wat een naslag inhoudt en weet waarmee hij al dan niet instemt. In sommige gevallen zal echter de instemming van betrokkene achterwege kunnen blijven en wel indien dit de effectiviteit van het uitvoeren van een verzoek kan schaden; artikel 50, derde lid, biedt hiervoor de mogelijkheid. In artikel 50, vierde lid, is ten slotte geregeld wie uiteindelijk de mededeling kan doen aan degene die het verzoek om naslag heeft gedaan. Hierbij is als uitgangspunt gekozen voor mededeling door de voor de desbetreffende dienst verantwoordelijke minister, zij het dat in bepaalde gevallen – mits voorzien in de regeling als bedoeld in artikel 8, tweede lid, onder f, of 10, tweede lid, onder g – dit ook namens de minister door het hoofd van de dienst kan plaatsvinden. Dit laatste kan met name wenselijk zijn indien het gaat om naslag naar kandidaat-bewindslieden van een nieuw te vormen kabinet, al is het alleen maar om de schijn van beïnvloeding te voorkomen van een zittende minister. Dat neemt overigens niet weg dat de naslag wel onder diens verantwoordelijkheid plaatsvindt.

Artikel 51: de derde partij-regel

In artikel 51, eerste lid, wordt bepaald dat de verstrekking van gegevens kan geschieden onder de voorwaarde dat degene aan wie de gegevens worden verstrekt, deze gegevens niet aan anderen mag verstrekken. Deze voorwaarde staat bekend als de derde-partij-regel (ook wel: *third party principle*). Deze moet overigens worden onderscheiden van het derde-landbeginsel (*third country principle*). Ingeval van de derde partijregel mag de

[86] Zoals dat thans plaatsvindt met betrekking tot onder meer kandidaat bewindslieden, waarbij het in het gesprek met de formateur aan de orde komt, en kandidaat burgemeesters, waarbij in de vacatureomschrijving melding wordt gemaakt dat naslag bij de AIVD onderdeel uitmaakt van het selectieproces.

partij die de gegevens verstrekt heeft gekregen, deze niet zonder toestemming van de verstrekkende instantie aan een andere partij – ook niet binnen hetzelfde land – verstrekken; bij een derde landbeginsel is dat laatste wel mogelijk, zij het dat natuurlijk wel geldt dat die verdere verstrekking in overeenstemming moet zijn met het doel waarvoor de gegevens zijn verstrekt (dit wordt dan bijvoorbeeld tot uitdrukking gebracht door een toevoeging als "*for intelligence use only*"). In artikel 51, tweede lid, is bepaald dat de derde-partijregel altijd moet worden gesteld bij verstrekking van gegevens aan buitenlandse collega-diensten als bedoeld in artikel 49, eerste lid, onder d. In artikel 77, derde lid, van het wetsvoorstel is (onder meer) artikel 51 van overeenkomstige toepassing verklaard, waar het gaat om gegevensverstrekking aan buitenlandse collega-diensten als bedoeld in artikel 77, eerste lid.

De derde-partijregel vormt een essentiële voorwaarde bij de internationale samenwerking. Inlichtingen- en veiligheidsdiensten moeten over en weer van elkaar op aan kunnen dat gegevens die zij onderling verstrekken – met inachtneming van de ter zake gemaakt afspraken – geheim worden gehouden. Als een dienst er niet van op aan kan, dat een gegeven door een dienst aan wie het is verstrekt geheim wordt gehouden ten behoeve van de eigen informatiepositie kan er van werkelijke samenwerking tussen de betreffende diensten geen sprake zijn. Indien bij een dienst de indruk ontstaat dat de regel niet wordt nageleefd, dan zal de informatie-uitwisseling met de desbetreffende collega-dienst worden stopgezet of gemarginaliseerd. Het is evident dat mede gelet op het feit dat het internationale karakter van dreigingen eerder toe- dan af zal nemen, samenwerking tussen de diensten van essentieel belang is om een adequate informatiepositie te verwerven en te behouden. De gegevens die door de internationale samenwerking worden verkregen, bieden de diensten de mogelijkheid om risico's voor de nationale veiligheid beter in kaart te brengen en de verantwoordelijke autoriteiten hiervoor te waarschuwen. In dit verband geldt hoe beter de internationale informatiepositie van een dienst hoe adequater en professioneler de informatievoorziening aan de nationale autoriteiten die bevoegd zijn tot het treffen van maatregelen. Wat aan het voor internationale samenwerking benodigde vertrouwen tevens bijdraagt is het feit dat de wettelijke geregelde zorgplicht tot bronbescherming (artikel 20 van het wetsvoorstel) ook voor buitenlandse collega-diensten (als internationale bronnen) geldt.

In artikel 51, derde lid, is ten slotte de mogelijkheid geopend dat in de gevallen dat gegevens onder toepassing van de derde-partijregel zijn verstrekt, door de voor de dienst verantwoordelijke minister of namens deze het hoofd van de dienst alsnog toestemming aan de geadresseerde van de verstrekte gegevens kan worden verleend om deze aan andere personen of instanties te verstrekken. Zo kan een buitenlandse collega-

dienst alsnog toestemming worden verleend om bepaalde gegevens die men van de AIVD of MIVD heeft verkregen verder te verstrekken. Wel kunnen aan die toestemming voorwaarden worden verbonden, zoals over de aard en het doel van het gebruik.

Artikel 52: ambtsberichten aan het openbaar ministerie

Artikel 52 van het wetsvoorstel geeft een regeling voor het verstrekken van door de diensten verwerkte gegevens die mogelijk van belang kunnen zijn voor de opsporing of vervolging van strafbare feiten aan het openbaar ministerie (ook wel: het uitbrengen van ambtsberichten aan het openbaar ministerie); een vergelijkbare bepaling is thans opgenomen in artikel 38 Wiv 2002. Bij onderzoeken van de diensten komt het meer dan eens voor dat men daarbij tevens stuit op strafbare feiten. Het zou echter aan een goede taakuitvoering door de diensten in de weg staan, indien men van elk strafbaar feit waarvan men kennisneemt, verplicht mededeling zou moeten doen aan het openbaar ministerie. Dat zou immers ertoe kunnen leiden dat ingeval het openbaar ministerie tot opsporing en vervolging daarvan overgaat, onderzoeken van de dienst kunnen worden gefrustreerd; dergelijke onderzoeken hebben veelal een langlopend karakter en de opbouw van een goede informatiepositie jegens onderzoekssubjecten vergt veelal veel tijd. Vandaar dat in artikel 52, eerste lid, van het wetsvoorstel, evenals in het huidige artikel 38, eerste lid, Wiv 2002, is bepaald dat een dergelijke mededeling aan het openbaar ministerie *kan* worden voldaan; het betreft met andere woorden een discretionaire bevoegdheid. Aan de desbetreffende minister is derhalve de ruimte gelaten om ter zake een eigen afweging te maken, zij het dat indien er sprake is van ernstige misdrijven, de ruimte om te beslissen geen mededeling te doen uitermate klein – zo niet nihil – wordt.[87] Maar in algemene zin geldt dat indien het belang van de dienst zich tegen aangifte verzet, dat belang prevaleert boven dat van opsporing en vervolging van strafbare feiten.[88] Echter de thans in artikel 38, eerste lid, Wiv 2002 opgenomen bepaling dat een en ander geldt "onverminderd dat daartoe een wettelijke verplichting bestaat" – lees: de plicht tot het doen van aangifte bij het openbaar ministerie ex artikel 162 Wetboek van Strafvordering (WvSv) – staat met voormeld uitgangspunt op gespannen voet. De CTIVD heeft in rapport nr. 9a (2005) aangegeven dat naar haar oordeel de tekst van artikel 38 Wiv 2002 geen ruimte laat voor een nuancering als door de regering bij de parlementaire behandeling van de Wiv 2002 is aangegeven. In reactie daarop is indertijd door de Minister van BZK aangegeven dat de conclusie van de CTIVD dat in voorkomende gevallen de wet geen ruimte biedt om af te zien van het doen van aangifte, dit ertoe leidt dat er een conflict van rechtsplichten optreedt. Dit kan bijvoorbeeld aan de

[87] Zie ook Kamerstukken II 1997/98, 25 877, nr. 3, blz. 58.
[88] Ook de Wet afgeschermde getuige gaat ervan uit dat het belang van de nationale veiligheid onder omstandigheden zwaarder kan wegen dan het belang van strafvordering.

orde zijn indien de AIVD kennis draagt van een ambtsmisdrijf en aangifte daarvan de bron daarvan in gevaar kan brengen; de plicht tot aangifte ex artikel 162 WvSv komt dan tegenover de wettelijke plicht tot bronbescherming te staan. Dan moet er afweging van rechtsplichten worden gemaakt. Deze afweging is vergelijkbaar met de afweging die ook dient plaats te vinden ingeval een ambtenaar die betrokken is bij de uitvoering van de wet, krachtens een wettelijke bepaling verplicht wordt als getuige of deskundige op te treden, en waarbij deze slechts een verklaring mag afleggen omtrent datgene waartoe zijn verplichting tot geheimhouding zich uitstrekt, voor zover de voor de desbetreffende minister en de Minister van Veiligheid en Justitie gezamenlijk hem daartoe schriftelijk van de verplichting hebben ontheven (zie artikel 86, tweede lid, Wiv 2002; artikel 125, tweede lid, van het wetsvoorstel). Om de hiervoor geconstateerde spanning weg te nemen is dan ook in voorliggend wetsvoorstel ervan afgezien de zinsnede "onverminderd dat daartoe een wettelijke verplichting bestaat" opnieuw op te nemen.[89]

Een mededeling als bedoeld in artikel 52, eerste lid, vindt plaats aan het daartoe aangewezen lid van het openbaar ministerie. In de praktijk is dit de Landelijk Officier van Justitie belast met terrorismebestrijding (LOvJ). Daarmee hebben de diensten één aanspreekpunt, hetgeen een efficiënte werkwijze bevordert; de LOvJ draagt vervolgens zorg voor verdere doorgeleiding binnen het openbaar ministerie. In de praktijk vindt over het algemeen voorafgaand aan het uitbrengen van een mededeling overleg plaats met de LOvJ. Dat overleg strekt er met name toe om vast te stellen of de informatie ook bruikbaar is voor het openbaar ministerie. De mededeling aan de hiervoor genoemde functionaris geschiedt schriftelijk, zij het dat in artikel 52, tweede lid, erin is voorzien dat in spoedeisende gevallen deze ook mondeling kan plaatsvinden. De mondelinge mededeling dient dan wel zo spoedig mogelijk schriftelijk te worden bevestigd.

Indien een mededeling aan het openbaar ministerie wordt gedaan kan dat ertoe leiden dat tot opsporing en vervolging wordt overgegaan; bovendien kan de informatie in een ambtsbericht ook bijdragen aan het bewijs in een strafzaak. Gelet op de mogelijk verstrekkende gevolgen die aan een dergelijke mededeling kunnen worden verbonden is in artikel 52, derde lid, erin voorzien dat op een daartoe strekkend verzoek van voornoemde LOvJ inzage wordt gegeven in *alle* aan de desbetreffende mededeling ten grondslag liggende gegevens die voor de beoordeling van de juistheid van de mededeling noodzakelijk zijn. Er bestaat in dit geval dus een verplichting om de desbetreffende gegevens ter inzage te geven. De artikelen 124 en 125 van het wetsvoorstel, waarin specifieke geheimhoudingsverplichtingen zijn neergelegd, zijn daarbij van

[89] Het schrappen van deze zinsnede was reeds voorzien in het ingetrokken post-Madridwetsvoorstel. Zie Kamerstukken II 2006/07, 30 553, nr. 8, onderdeel B; Kamerstukken I 2007/08, 30 553, A, Artikel I, onderdeel Pa.

overeenkomstige toepassing verklaard. De LOvJ kan in dit kader dan bezien of de inhoud van de mededeling gedragen wordt door de achterliggende stukken en ook of de betrouwbaarheidsaanduiding juist is. Het is echter niet aan de LOvJ om de rechtmatigheid van de gegevensverzameling die ten grondslag ligt aan het ambtsbericht alsmede het waarheidsgehalte van de informatie in het ambtsbericht te controleren.

Artikel 53: verstrekking op grond van een dringende en gewichtige redenen

Artikel 53, eerste lid, van het wetsvoorstel biedt, evenals het huidige artikel 39, eerste lid, Wiv 2002, de mogelijkheid om indien bij de verwerking van gegevens door of ten behoeve van een dienst daarvan is gebleken, op grond van een dringende of gewichtige reden schriftelijk mededeling te doen aan bij of krachtens algemene maatregel van bestuur aangewezen personen of instanties die betrokken zijn bij de uitvoering van de publieke taak, voor zover deze gegevens tevens van belang kunnen zijn voor de behartiging van de aan hen in dat kader opgedragen belangen. Het gaat hierbij om een verstrekking die plaatsvindt anders dan in het kader van de uitvoering van de aan de diensten in artikel 8 en 10 opgedragen taken.[90] Bij deze verstrekking staat het belang van de persoon of instantie waaraan de mededeling wordt gedaan centraal. Zonder een wettelijke regeling ter zake zou, gelet op het gesloten verstrekkingenstelsel, een dergelijke verstrekking niet mogelijk zijn.

Op grond van het eerste lid is het Aanwijzingsbesluit artikel 39 WIV 2002 tot stand gebracht, waarin limitatief de personen en instanties zijn aangewezen, waaraan een verstrekking als hier bedoeld mag plaatsvinden. Naast de ministers, betreft het de Nederlandsche Bank N.V., de Stichting Autoriteit Financiële Markten en de burgemeesters, voor zover het betreft hun taak als bedoeld in artikel 172, eerste lid, van de Gemeentewet alsmede voor zover het betreft hun taak betreffende het adviseren omtrent voorstellen voor het verlenen van een Koninklijke onderscheiding. Al met al een beperkte kring van geadresseerden, hetgeen in lijn is met de indertijd bij de parlementaire behandeling van artikel 39 Wiv 2002 uitgesproken mening dat van deze bevoegdheid een terughoudend gebruik gemaakt moest worden, hetgeen zich ook heeft vertaald in de eis dat het moet gaan om een dringende en gewichtige reden.

In artikel 53, tweede lid, is artikel 54, tweede en derde lid, van overeenkomstige toepassing verklaard. Kortheidshalve wordt verwezen naar hetgeen verderop in de toelichting daaromtrent is opgemerkt.

[90] Overigens zal ook bij een verstrekking als bedoeld in artikel 52 van het wetsvoorstel (ambtsbericht aan het openbaar ministerie) het doorgaans gaan om een verstrekking die niet voortvloeit uit een van de aan de diensten opgedragen taken, maar om exploitatie van zogeheten bijvangst.

Tot slot is in het derde lid voorzien in een voorhangprocedure met betrekking tot de op grond van het eerste lid vast te stellen algemene maatregel van bestuur.

3.3.5.3.2 Bijzondere bepalingen betreffende de externe verstrekking van persoonsgegevens

In paragraaf 3.4.2.2 (artikelen 54 tot en met 56) worden enkele bijzondere bepalingen gegeven waar het gaat om de verstrekking van persoonsgegevens. Thans vindt men deze bepalingen terug in paragraaf 3.3.2.2 (artikelen 40 tot en met 42) van de Wiv 2002. Zoals indertijd ter toelichting is aangegeven[91], is de ratio hiervan, dat meer nog dan al het geval is bij verstrekking van gegevens in zijn algemeenheid door de diensten, bij de verstrekking van persoonsgegevens die zeer nadrukkelijk de persoonlijke levenssfeer raken van degene waarop die gegevens betrekking hebben, zorgvuldigheid voorop dient te staan. Zeker nu met verstrekking van gegevens door de diensten in het kader van hun taakuitvoering veelal wordt beoogd een geconstateerde dreiging weg te nemen dan wel te verkleinen. Als de dreiging afkomstig is van een bepaalde persoon, zal de verstrekking van op hem betrekking hebbende gegevens er in de praktijk toe kunnen leiden dat er maatregelen jegens hem worden getroffen. Mede met het oog op dit laatste zijn in artikel 54 van het wetsvoorstel enkele waarborgen opgenomen met betrekking tot de verstrekking van persoonsgegevens aan personen en instanties die naar aanleiding van een mededeling van de dienst bevoegd zijn jegens de persoon waarop de mededeling betrekking heeft bepaalde maatregelen te treffen. Een eerste waarborg is daarin gelegen, dat ingevolge artikel 54, eerste lid, in dergelijke gevallen persoonsgegevens schriftelijk dienen te worden medegedeeld. Uitsluitend in spoedeisende gevallen kan de mededeling mondeling plaatsvinden, echter de desbetreffende minister of namens deze het hoofd van de dienst dient de mededeling zo spoedig mogelijk schriftelijk te bevestigen. In artikel 54, derde lid, is tot slot een grotendeels met artikel 52, derde lid, vergelijkbare regeling opgenomen. De desbetreffende persoon of namens deze het hoofd van de dienst kan aan de persoon of instantie waaraan de mededeling is gedaan inzage verlenen aan de aan de mededeling ten grondslag liggende stukken, voor zover dat voor de beoordeling van de juistheid van de mededeling noodzakelijk is. Het betreft in tegenstelling tot hetgeen in artikel 52, derde lid, is bepaald geen verplichting maar een discretionaire bevoegdheid. Met betrekking tot de personen en instanties waaraan inzage is verleend in de onderliggende stukken zijn de bijzondere geheimhoudingsbepalingen, zoals neergelegd in de artikelen 124 en 125, tweede en derde lid, van overeenkomstige toepassing. Anders dan bij artikel 52, is artikel 125, eerste lid, hier niet van overeenkomstige toepassing verklaard; dat

[91] Zie Kamerstukken II 1997/98, 25 877, nr. 3, blz. 59.

betekent dat een bovengestelde van de ambtenaar die inzage heeft verkregen, deze niet van diens geheimhoudingsverplichting tegenover hem in dezen kan ontslaan. In het kader van ambtsberichten die aan het openbaar ministerie worden uitgebracht en waarbij de LOvJ inzage in de onderliggende stukken heeft gekregen, kan het echter wenselijk zijn dat deze gelet op de aard van de informatie en de eventueel naar aanleiding daarvan te nemen vervolgstappen in de gelegenheid is daarover overleg te voeren met bijvoorbeeld een lid van het college van procureurs-generaal; op grond van artikel 125, eerste lid, kan deze dan de LOvJ van diens geheimhoudingsverplichting tegenover hem ontslaan.

Artikel 55 geeft aansluitend een regeling voor de gevallen waarin er geen persoonsgegevens (meer) mogen worden verstrekt (eerste lid); daarbij wordt echter tevens voorzien in een beperkt aantal mogelijkheden om van die regeling af te wijken, zij het wel omgeven met enkele waarborgen (tweede tot en met vierde lid). Allereerst mogen er geen persoonsgegevens worden verstrekt waarvan de juistheid redelijkerwijs niet kan worden vastgesteld. Hiervan zal bijvoorbeeld sprake zijn in het geval van in het kader van een niet-regulier samenwerkingsverband door derden aan de diensten verstrekte persoonsgegevens, waarvan de diensten niet eigenstandig kunnen vaststellen dat het betrouwbare, correcte persoonsgegevens betreft. In dergelijke gevallen wordt het onwenselijk geacht deze persoonsgegevens vanuit de diensten aan derden te laten verstrekken. Met het begrip ‘redelijkerwijs’ wordt gedoeld op de inspanningsplicht die de diensten hebben om de juistheid vast te stellen. Daarnaast mogen geen persoonsgegevens worden verstrekt die meer dan 10 jaar geleden zijn verwerkt, terwijl ten aanzien van de desbetreffende persoon sindsdien geen nieuwe gegevens zijn verwerkt. Het gaat dan immers om personen die al meer dan 10 jaar niet meer in de aandachtssfeer van de dienst zijn gekomen. Verstrekking van dergelijke gegevens dient dan geen enkel redelijk doel meer. Er kunnen zich echter wel een aantal situaties voor doen dat verstrekking van de hiervoor bedoelde persoonsgegevens wel dient plaats te vinden. In artikel 55, tweede lid, is daarbij voor een drietal situaties de mogelijkheid geschapen. In artikel 55, tweede lid, aanhef en onder a, is allereerst bepaald dat in afwijking van het eerste lid verstrekking mogelijk is aan daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen, alsmede daarvoor in aanmerking komende internationale beveiligings-, verbindingsinlichtingen- en inlichtingenorganen. Het feit dat een persoon niet meer in de aandachtssfeer van de AIVD of MIVD bevindt, wil nog niet zeggen dat hij zich niet in de aandachtssfeer van een buitenlandse collega-dienst kan bevinden. De omtrent hem beschikbare informatie bij de AIVD of MIVD kan in voorkomende gevallen voor die buitenlandse collega-dienst van belang zijn bij het onderzoek dat door die collega-dienst wordt verricht. In dat geval biedt de regeling dus de mogelijkheid om van de desbetreffende persoonsgegevens

mededeling te doen aan die dienst, zij het dat daarbij ingevolge het bepaalde in het derde lid zowel dient te worden aangegeven wat de mate van betrouwbaarheid als wat de ouderdom van de aan de mededeling ten grondslag liggende gegevens is. Voor zover door betrokkene in het kader van het door hem uitgeoefende recht op kennisneming met betrekking tot de desbetreffende gegevens door hem een verklaring als bedoeld in artikel 65, eerste lid, is afgelegd die vervolgens bij diens persoonsgegevens is gevoegd, dient ook deze verklaring te worden verstrekt. Een tweede uitzondering op de in het eerste lid neergelegde regeling betreft de mogelijkheid tot het doen van een mededeling aan instanties die zijn belast met de opsporing en vervolging van strafbare feiten (artikel 55, tweede lid, aanhef en onder b). Daarnaast kan door de betrokken minister ook aan andere instanties – dus buiten de kring van inlichtingen- en veiligheidsdiensten en opsporingsinstanties – in bijzonder gevallen een mededeling van de hier bedoelde gegevens doen. Ook in deze twee andere situaties dient het bepaalde in het derde lid in acht te worden genomen. Tot slot is in het vierde lid voorzien in het van overeenkomstige toepassing verklaren van artikel 54, derde lid. Zoals reeds eerder is aangegeven, biedt dat artikel de moegelijkheid om inzage te verlenen in de aan de mededeling ten grondslag liggende gegevens voor zover dat noodzakelijk is om de juistheid van de mededeling te kunnen vaststellen. Zeker in de gevallen dat het gaat om gegevens ouder dan 10 jaar en welke (mede) de grondslag kunnen vormen om jegens de betrokkene (alsnog) maatregelen te treffen, moet de mogelijkheid bestaan om – mede met het oog op een zorgvuldige besluitvorming ter zake – de juistheid van de mededeling aan de hand van de achterliggende gegevens te toetsen.

In artikel 56 is ten slotte bepaald dat van de verstrekking van persoonsgegevens aantekening dient te worden gehouden. Het is van groot belang dat de diensten hier de hand aan houden en dat deze aantekening ook zodanig accuraat is, dat daarmee een effectieve controle op de rechtmatigheid van de verstrekking door de CTIVD mogelijk is. Voorts is dit van belang om in het geval dat achteraf blijkt dat de verstrekte gegevens onjuist zijn of ten onrechte door de dienst zijn verwerkt, aan de instanties waaraan de gegevens zijn verstrekt daarvan mededeling kan worden gedaan; artikel 57, tweede lid, verplicht daartoe.

3.3.6 De verwijdering, vernietiging en overbrenging van gegevens

In paragraaf 3.5 (de artikelen 57 en 58) van het wetsvoorstel zijn enkele bepalingen opgenomen inzake de verwijdering, vernietiging en overbrenging van gegevens. Het betreft hier een bestaande regeling die in het wetsvoorstel ongewijzigd is overgenomen.

In algemene zin geldt dat gegevens, die gelet op het doel waarvoor zij worden verwerkt, hun betekenis hebben verloren, dienen te worden verwijderd (artikel 57, eerste lid).

Verwijderen wil zeggen dat de gegevens niet langer toegankelijk zijn voor het reguliere bedrijfsproces (dat wil zeggen ten behoeve van de taakuitvoering van de diensten); zij dienen daarvan te worden afgezonderd.[92] Wel blijven de verwijderde gegevens beschikbaar voor archiefdoeleinden, klachtbehandeling e.d. Dit in tegenstelling tot vernietigen waarbij de gegevens definitief en onomkeerbaar uit de systemen waarin dan wel van de gegevensdragers waarop ze zijn vastgelegd verdwijnen. Verwijderde gegevens kunnen daarom, vanwege het feit dat ze nog niet zijn vernietigd, onder omstandigheden toch weer opnieuw gebruikt worden, indien het doel waarvoor ze aanvankelijk waren verworven weer actueel is geworden of voor een eventueel ander doel, mits uiteraard wordt voldaan aan de aan eisen die in algemene zin aan gegevensverwerking worden gesteld. Waar het gaat om verwijderde gegevens zal het vaak ook gaan om gegevens die inmiddels wat ouder zijn; dit gegeven – mede gelet op het bepaalde in artikel 55 van het wetsvoorstel – dient nadrukkelijk bij de beslissing over (verder) gebruik betrokken te worden. Indien blijkt dat gegevens onjuist zijn of ten onrechte worden verwerkt, dienen deze te worden verbeterd onderscheidenlijk verwijderd; aan de personen of instanties waaraan de desbetreffende gegevens eerder zijn verstrekt moeten daarvan zo spoedig mededeling worden gedaan (artikel 57, tweede lid). Indien de desbetreffende persoon of instantie waaraan de gegevens eerder zijn verstrekt op basis van die informatie maatregelen heeft ondernomen jegens de persoon waarop de informatie betrekking heeft, wordt deze aldus in de gelegenheid gesteld om – indien dat noodzakelijk is – deze te heroverwegen. De verwijderde gegevens dienen te worden vernietigd, tenzij wettelijke regels omtrent bewaring hieraan in de weg staan. Met dit laatste wordt gedoeld op de Archiefwet 1995. In artikel 57, vierde lid, is ten slotte een regeling opgenomen, welke beoogt te garanderen dat de vernietiging van daarvoor in aanmerking komende gegevens wordt opgeschort indien ten aanzien van die gegevens een aanvraag als bedoeld in artikel 64 is gedaan. In dat geval wordt de vernietiging van de gegevens opgeschort tot ten minste het moment waarop op de aanvraag om kennisneming van de desbetreffende gegevens onherroepelijk is beslist. Voor zover de aanvraag om kennisneming is ingewilligd, worden de desbetreffende gegevens niet eerder vernietigd dan nadat de betrokkene van de desbetreffende gegevens overeenkomstig artikel 64, tweede lid, kennis heeft kunnen nemen. Aldus wordt voorkomen dat gegevens hangende een aanvraag tot kennisneming daarin worden vernietigd, waarmee het recht op kennisneming illusoir zou worden gemaakt.

Artikel 58 van het wetsvoorstel geeft een bijzondere regeling voor de overbrenging van archiefbescheiden naar een archiefbewaarplaats. Deze regeling is ten opzichte van de

[92] Bij de AIVD worden de verwijderde gegevens verplaatst naar een semistatisch archief, waar de gegevens slechts voor een beperkt aantal medewerkers toegankelijk zijn.

bestaande regeling ongewijzigd gebleven. Ter zake is indertijd ter toelichting het volgende opgemerkt.[93] In de in artikel 58 opgenomen regeling wordt gekozen voor een ietwat andere bendering dan die welke op grond van de Archiefwet 1995 met betrekking tot de archiefbescheiden van de diensten voortvloeit. Op basis van artikel 12 van de Archiefwet 1995 dienen daarvoor in aanmerking komende archiefbescheiden die ouder zijn dan twintig jaar te worden overgebracht naar een archiefbewaarplaats. Deze verplichting kan ingevolge artikel 13, derde lid, van de Archiefwet 1995 worden opgeschort, indien de desbetreffende archiefbescheiden door het betrokken overheidsorgaan nog veelvuldig worden gebruikt of geraadpleegd. Wordt niet aan deze voorwaarde voldaan, dan is overbrenging aangewezen. Artikel 18, eerste lid, biedt dan echter de mogelijkheid om de desbetreffende archiefbescheiden voor een bepaalde tijd «terug te lenen». Op deze wijze kan worden voorkomen dat de desbetreffende archiefbescheiden fysiek buiten het bereik van het betrokken overheidsorgaan geraken. In de gevallen waar het gaat om archiefbescheiden van één van de diensten (of de coördinator) zullen de desbetreffende gegevens altijd worden teruggeleend, zolang met betrekking tot die archiefbescheiden de geheimhouding in verband met onder meer de veiligheid van de staat nog niet is opgeheven. Voor de duur dat de geheimhouding niet is opgeheven dienen deze archiefbescheiden niet buiten het bereik van de diensten te worden gebracht en derhalve bij deze te blijven berusten. Dat heeft bovendien ook praktische redenen, zoals bijvoorbeeld om verzoeken om kennisneming van gegevens op grond van hoofdstuk 5 van het wetsvoorstel adequaat te kunnen behandelen. Daarnaast zijn de beveiligingsmaatregelen van de diensten met betrekking tot de bij hen berustende gegevens toegesneden op de aard van die gegevens en kunnen alleen die personen daarmee in aanraking komen die daartoe zijn aangewezen. Dit laatste in verband met het eerder in deze memorie besproken «need-to-know»-principe.

De constructie van «terug lenen» van archiefbescheiden is in deze situatie dan ook minder fraai. Vandaar dat wordt voorgesteld de overbrenging op te schorten, in die zin dat slechts die archiefbescheiden worden overgebracht naar een archiefbewaarplaats die ouder zijn dan twintig jaar en waarvan door de betrokken minister, na advies van de beheerder van die archiefbewaarplaats, is vastgesteld dat daaraan geen beperkingen aan de openbaarheid dienen te worden gesteld met het oog op het belang van de staat of diens bondgenoten (artikel 58, eerste lid). De adviserende rol van de beheerder van de archiefbewaarplaats is van betekenis om langs deze weg te bewerkstelligen dat de belangen die aan de Archiefwet 1995 ten grondslag liggen, met name waar het gaat om de goede zorg voor archieven, nadrukkelijk in de besluitvorming van de betrokken minister worden betrokken.

[93] Zie Kamerstukken II 1997/98, 25 877, nr. 3, blz. 61.

In artikel 58, tweede lid, is voorts bepaald dat de beperkingen die aan de openbaarheid kunnen worden gesteld met het oog op het belang van de staat of diens bondgenoten geen betrekking hebben op archiefbescheiden die ouder zijn dan vijfenzeventig jaar, tenzij de betrokken minister, in overeenstemming met het gevoelen van de ministerraad, anders beslist. Het betreft hier een regeling die ook in de Archiefwet 1995 is opgenomen, zij het dat de regeling daar is beperkt ten aanzien van archiefbescheiden die inmiddels zijn overgebracht naar een archiefbewaarplaats (artikel 15, vierde lid jo. zesde lid, van de Archiefwet 1995). Er is geen reden om die regeling ook niet te doen gelden ten aanzien van archiefbescheiden die op grond van artikel 58, eerste lid, nog bij de diensten berusten.

Hoofdstuk 4 Overige bijzondere bevoegdheden van de diensten

4.1 Algemeen

Het wetsvoorstel voorziet ten opzichte van de huidige wet in een nieuw hoofdstuk, te weten hoofdstuk 4. In het ingetrokken post-Madridwetsvoorstel was reeds in een dergelijke aanpassing voorzien. In hoofdstuk 4 van het wetsvoorstel zijn twee bepalingen opgenomen die in materiële zin thans reeds in paragraaf 3.2.2 van de Wiv 2002 voorkomen, maar die anders dan de overige in die paragraaf geregelde bijzondere bevoegdheden niet gericht zijn op het verzamelen van gegevens. Vanuit wetstechnisch oogpunt bezien dient een zuiver onderscheid te worden gemaakt tussen enerzijds bijzondere bevoegdheden die wel en bijzondere bevoegdheden die niet zijn gericht op het verzamelen van gegevens. Daarbij komt dat niet alle vereisten die zijn gesteld aan de verwerking van gegevens van toepassing kunnen zijn op deze bijzondere bevoegdheden.

De bijzondere bevoegdheden die niet zien op de verzameling van gegevens betreffen de bevoegdheid tot het oprichten en de inzet van rechtspersonen en de bevoegdheid tot het bevorderen of treffen van maatregelen. Bij het aanbrengen van het hiervoor aangeduide onderscheid is bezien welke artikelen uit paragraaf 3.2.2 op de uitoefening van de bevoegdheden die in hoofdstuk 4 worden opgenomen, van overeenkomstige toepassing dienen te worden verklaard. Het betreft hier de bepalingen die betrekking hebben op de specifieke taak waarvoor de bevoegdheden mogen worden ingezet (artikel 23), het toestemmingsvereiste (artikel 24) alsmede de bepaling betreffende de verslaglegging van de uitoefening van de bevoegdheid (artikel 45). Artikel 59 voorziet daarin.

4.2 De oprichting en inzet van rechtspersonen

In artikel 60 is de bevoegdheid voor de diensten neergelegd om ter voorbereiding op en ondersteuning van operationele activiteiten rechtspersonen op te richten en in te zetten. Dit artikel is op enkele punten gewijzigd ten opzichte van hetgeen thans in artikel 21, eerste lid, onderdeel b, en achtste lid, van de Wiv 2002 is bepaald. Toegevoegd is in de eerste plaats dat de diensten ook *ter voorbereiding op* operationele activiteiten rechtspersonen mogen oprichten en inzetten. Het oprichten van een rechtspersoon is op zich geen ingewikkelde aangelegenheid en kan redelijk snel plaatsvinden, echter ten behoeve van een effectieve en geloofwaardige operationele inzet is het wenselijk om te voorzien in de mogelijkheid dat reeds rechtspersonen kunnen worden opgericht voor operationele activiteiten die in de toekomst liggen. Voor het oprichten van de rechtspersoon is - zoals nu ook het geval is - de toestemming nodig van de betrokken minister of namens deze het hoofd van de desbetreffende dienst. Nieuw is verder het bepaalde in artikel 60, tweede lid. Daarin is bepaald dat de toestemming voor de inzet van een rechtspersoon wordt verleend voor de duur van het onderzoek waarbij de rechtspersoon wordt ingezet, met inbegrip van de periode die nodig is om tot een verantwoorde afbouw van de inzet in verband met het desbetreffende onderzoek te komen. Bij de inzet van een rechtspersoon in het kader van een onderzoek heeft de verplichting om telkens voor een periode van drie maanden toestemming te vragen immers geen toegevoegde waarde. Dat heeft deze nadrukkelijk wel waar het gaat om de inzet van bijzondere bevoegdheden als bedoeld in paragraaf 3.2.2 van de huidige wet, waarbij (veelal) een inbreuk plaatsvindt op het recht op bescherming van de persoonlijke levenssfeer van de personen die in onderzoek zijn van een dienst en waarbij het verzoek om (verlenging van de) toestemming nadrukkelijk aandacht moet worden besteed aan aspecten als subsidiariteit en proportionaliteit. Nu bij het oprichten en de inzet van rechtspersonen geen sprake is van een inbreuk op het recht op bescherming van de persoonlijke levenssfeer, zoals die wel bij de andere bijzondere bevoegdheden aan de orde kan zijn, is er van afgezien de artikelen 43, derde en vierde lid, en 44 van het wetsvoorstel van overeenkomstige toepassing te verklaren. De daarin neergelegde proportionaliteits- en subsidiariteitstoets is in casu niet aan de orde.

4.3 Het bevorderen of treffen van maatregelen

In artikel 61 wordt voorzien in de bevoegdheid tot het bevorderen of treffen van maatregelen ter bescherming van door een dienst te behartigen belangen. Ook deze bevoegdheid is thans in artikel 21 opgenomen. In artikel 21 van de Wiv 2002 is namelijk voorzien in de mogelijkheid om een “agent” te belasten met het bevorderen of treffen van maatregelen ter bescherming van door een dienst te behartigen belangen. Opgemerkt wordt dat deze bevoegdheid niet louter voor verstoring kan worden ingezet, maar ook anderszins. Het gaat er bij de toepassing van deze mogelijkheid met name om

bepaalde anti-democratische, staatsgevaarlijke activiteiten of andere activiteiten die gericht zijn tegen één van de andere in de wet genoemde belangen, te ontmoedigen of in de kiem te smoren met als doel te voorkomen (preventief) dat de met de genoemde activiteiten gepaard gaande risico's worden gerealiseerd. Maatregelen in de preventieve sfeer kunnen echter ook voorwaardenscheppend zijn voor het op een adequate wijze onder controle krijgen en houden van targets of dat bijzondere bevoegdheden die op de verzameling van gegevens zijn gericht op een (nog) effectieve(re) manier kunnen worden toegepast. De toepassing van deze bijzondere bevoegdheid is dan ook niet louter als *ultimum remedium* aan te merken.

De mogelijkheid tot het bevorderen of treffen van maatregelen is in artikel 21 van de huidige wet gekoppeld aan de inzet van een agent die daartoe een instructie krijgt, terwijl er echter ook mogelijkheden tot verstoring bestaan waarbij het niet noodzakelijk is dat daarbij een agent ingezet wordt. Met betrekking tot bijvoorbeeld verstoringsacties in de sfeer van internet kunnen immers reguliere medewerkers van de dienst worden ingezet. Vandaar dat wordt voorgesteld om in artikel 61 de mogelijkheid tot het bevorderen of treffen van maatregelen te formuleren als een bevoegdheid die de diensten als zodanig toekomt. Voorts is daarbij buiten kijf gesteld dat bij de toepassing van deze bijzondere bevoegdheid ook technische hulpmiddelen mogen worden aangewend. In het rapport van de Commissie bestuurlijke evaluatie AIVD (CBE), wordt de aanbeveling gedaan dat de procedure voor verstoring nauwkeuriger wordt omschreven. In het bijzonder geeft de CBE aan dat "bij een besluit zelf te verstoren of partners in de veiligheidsketen in te schakelen met het oog op het nadeel dat onschuldige derden door de verstoringsactie kunnen ondervinden rekening dient te worden gehouden met 1) de ernst van het risico (oftewel het product van de waarschijnlijkheid en de ernst van de dreiging); 2) de onmiddellijkheid van het risico; 3) de sterkte van de aanwijzingen dat de dreiging zal worden verwezenlijkt en 4) de impact die de verstoringsactie op de rechtstreeks betrokkene zal hebben". De Minister van BZK heeft indertijd in reactie op het rapport aangegeven, deze aanbeveling van de CBE over te willen nemen[94]. Bezien is op welke wijze dit het beste geïmplementeerd kan worden. Voor een deel kan dit plaats vinden door in artikel 61 het afwegingskader dat bij de toepassing van de bevoegdheid dient te worden gehanteerd op te nemen. Het gaat dan om een op de toepassing van deze bevoegdheid toegesneden subsidiariteits- en proportionaliteitstoets. Artikel 61, tweede lid, geeft daaraan invulling. Aldaar wordt bepaald dat bij het bevorderen of treffen van een maatregel slechts die maatregel wordt bevorderd of getroffen, die gelet op de omstandigheden van het geval, waaronder de ernst van de bedreiging van de door de dienst te beschermen belangen, voor de

[94] Kamerstukken II, 2004-2005, 29 876, nr. 3, p. 3.

betrokkene – jegens wie de maatregel wordt bevorderd of getroffen – de minste nadeel oplevert. Voorts zijn de artikelen 43, derde en vierde lid, en 44 van overeenkomstige toepassing verklaard. Ingevolge artikel 43, derde lid, dient de uitoefening van de bevoegdheid achterwege te blijven, indien deze voor de betrokkene een onevenredig nadeel in vergelijking met het daarbij na te streven doel oplevert. Artikel 43, vierde lid, bepaalt aansluitend dat de uitoefening van de bevoegdheid evenredig dient te zijn aan het daarmee beoogde doel. Op grond van artikel 44 dient de uitoefening van een bevoegdheid onmiddellijk te worden gestaakt, indien het doel waartoe de bevoegdheid is uitgeoefend is bereikt dan wel met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan. De door de CBE in zijn aanbeveling genoemde aspecten zullen bij de toepassing van het hiervoor geschetste afwegingskader aan de orde komen en voorts zal in een interne procedureregeling – langs de in artikel 61 aangegeven lijnen - het bij de toepassing van deze bijzondere bevoegdheid te hanteren afwegingskader nader worden geoperationaliseerd.

In artikel 61, derde lid, is bepaald dat het bevorderen of treffen van maatregelen bij instructie kan worden opgedragen aan een natuurlijke persoon als bedoeld in artikel 26, eerste lid, van het wetsvoorstel. Hiermee wordt de thans bestaande mogelijkheid om een “agent” met dergelijke acties te belasten, bestendigd.

Bij het bevorderen of treffen van maatregelen is het niet uitgesloten dat daarbij strafbare feiten worden (mede)gepleegd. Voor zover dat door een natuurlijke persoon als bedoeld in artikel 26, eerste lid, dient te geschieden, voorziet artikel 26, derde tot en met zevende lid, in het daarbij in acht te nemen kader. Nu de toepassing van de bevoegdheid tot het bevorderen of treffen van maatregelen ook kan plaatsvinden door anderen dan de in artikel 26, eerste lid, bedoelde “agenten”, kan echter ook in die gevallen sprake zijn van de noodzaak tot het (mede)plegen van strafbare feiten, en dient daarvoor het in artikel 26, derde tot en met zevende lid, opgenomen kader ook in deze gevallen van overeenkomstige toepassing te worden verklaard. Artikel 61, vierde lid, voorziet daarin, waarbij tevens is bepaald dat onder “natuurlijke persoon” of “persoon” in de genoemde artikelleden dient te worden verstaan: de personen die door de dienst worden belast met het bevorderen of treffen van maatregelen als bedoeld in het eerste lid. Aldus wordt bewerkstelligd dat met inachtneming van de in artikel 26, derde tot en met zevende lid, opgenomen bepalingen, ook deze personen bij de uitvoering van de desbetreffende instructie – die aangemerkt moet worden als een bevoegd gegeven ambtelijk bevel – niet strafbaar zijn.

Hoofdstuk 5 Kennisneming van door of ten behoeve van de diensten verwerkte gegevens

5.1 Algemeen

De commissie Dessens heeft in haar rapport geconcludeerd dat het inzageregime van hoofdstuk 4 van de Wiv 2002 duidelijke verbeteringen bevat ten opzichte van de regeling die vóór de inwerkingtreding van de huidige wet gold, maar dat er nog wel een aantal knelpunten bestaan.[95] Zo beveelt de commissie aan dat er een leidraad wordt opgesteld waarin geregeld wordt hoe een verzoekschrift moet worden geformuleerd en welke gegevens opgevraagd kunnen worden. Het kabinet heeft in reactie hierop aangegeven dat zij zich in deze aanbeveling kan vinden. Het kabinet acht het van groot belang dat hiermee vanuit het oogpunt van transparantie en voorzienbaarheid de informatievoorziening aan de burger kan worden versterkt. De opinies van de CTIVD betreffende inzageverzoeken en de uitleg van de bepalingen in de Wiv 2002 door de CTIVD op dat gebied zullen in de leidraad worden verwerkt. De commissie doet ten slotte de aanbeveling om in de wet alsnog een correctierecht op te nemen. Het kabinet heeft aangegeven deze aanbeveling niet over te nemen; de thans bestaande mogelijkheid tot het overleggen van een verklaring ex artikel 48 Wiv 2002 komt immers materieel gezien daarmee overeen.[96]

Nu naar aanleiding van de evaluatie van de Wiv 2002 noch anderszins geen aanleiding bestaat om de regeling inzake kennisneming van persoonsgegevens en andere gegevens te herzien, is deze ongewijzigd overgenomen in hoofdstuk 5 van het wetsvoorstel. In verband daarmee zal in de toelichting regelmatig worden gerefereerd aan hetgeen indertijd ter toelichting op de thans geldende regeling tijdens de parlementaire behandeling naar voren is gebracht.

Zoals eerder in deze memorie van toelichting naar voren is gebracht kent de wet een gesloten verstrekkingenstelsel, waartoe ook de regeling inzake kennisneming van gegevens moet worden gerekend. In artikel 62 van het wetsvoorstel is dit tot uitdrukking gebracht. Dat betekent onder meer dat de Wet openbaarheid van bestuur (Wob) niet van toepassing is op het kennisnemen van de door of ten behoeve van de diensten en de coördinator verwerkte gegevens. Wel is bij de uitwerking van de regeling op diverse onderdelen – al dan niet in aangepaste vorm - aansluiting gezocht bij onderdelen van de Wob, waaronder de uitleg van enkele begrippen (artikel 63 van het wetsvoorstel) en de regeling inzake weigeringsgronden en beperkingen (paragraaf 5.5. van het wetsvoorstel). In de regeling wordt een onderscheid gemaakt in kennisneming van persoonsgegevens (paragraaf 5.2) en in kennisneming van andere gegevens dan persoonsgegevens (paragraaf 5.3). Dit onderscheid is gemaakt, aangezien de persoonsgegevens die door de

[95] Rapport van de commissie Dessens, par. 7.2.7 (blz. 141).
[96] Kamerstukken II 2013/14, 33 820, nr. 2, blz. 7-8.

diensten zijn verwerkt met het oog op een goede taakuitoefening over het algemeen een grotere mate van geheimhouding vergen dan andere gegevens die door of ten behoeve van de diensten zijn verwerkt. Openbaarmaking van persoonsgegevens, zeker indien die zicht zou geven op het actuele kennisniveau van de dienst, zoals bijvoorbeeld het gegeven dat betrokkene wordt aangemerkt als iemand die gelieerd is aan een terroristische organisatie, draagt het risico in zich dat betrokkene zijn gedrag daarop gaat aanpassen, waardoor onderzoeken van de dienst kunnen worden gefrustreerd.

5.2 Recht op kennisneming van persoonsgegevens

5.2.1 Algemeen

Het recht op kennisneming van persoonsgegevens komt in het wetsvoorstel toe aan de betrokkene zelf (artikel 64, eerste lid) alsmede aan personen ten opzichte van wie de betrokkene in een bijzondere relatie stond, te weten die van overleden echtgenoot, geregistreerd partner, kind of ouder van de aanvrager (artikel 67, eerste lid). Laatstgenoemde regeling was aanvankelijk in het indertijd ingediende wetsvoorstel niet voorzien, aangezien aan de kennisnemingsregeling het uitgangspunt ten grondslag lag dat derden geen inzage in persoonsgegevens zouden moeten kunnen krijgen. Op verzoek van de Tweede Kamer is deze voor een beperkte en nauw afgebakende kring van derden alsnog in de wet opgenomen.[97] De (emotionele) betrokkenheid van familieleden bij het wel en wee van degene omtrent wie (vermoedelijk) gegevens bij een dienst zijn geregistreerd achtte de regering een voldoende overtuigend argument om voor deze – nader omschreven – categorie van derden een mogelijkheid tot inzage in persoonsgegevens te openen.[98] Een en ander betekent dat andere personen dan hier bedoeld geen inzage in persoonsgegevens kunnen vragen. Kennisneming van door of ten behoeve van de diensten verwerkte persoonsgegevens is voor hen pas mogelijk, indien deze op enig moment – onder toepassing van de op grond van de Archiefwet 1995 vast te stellen selectielijst - naar het Nationaal Archief zijn overgebracht.

5.2.2 Kennisneming van omtrent de aanvrager verwerkte persoonsgegevens

In artikel 64 van het wetsvoorstel (huidig artikel 47 Wiv 2002) is bepaald, dat de betrokken minister een ieder op diens aanvraag zo spoedig mogelijk, doch uiterlijk binnen drie maanden, mededeelt of en, zo ja, welke hem betreffende persoonsgegevens door of ten behoeve van een dienst zijn verwerkt. De betrokken minister kan zijn besluit voor ten hoogste vier weken verdagen, waarvan voor de afloop van de eerste termijn schriftelijk gemotiveerd mededeling aan de aanvrager wordt gedaan. De termijn van drie

[97] Kamerstukken II 2000/01, 25 877, nr. 15, onderdeel L.
[98] Kamerstukken II 2000/01, 25 877, nr. 14, blz. 49-50.

maanden (en na verlenging vier maanden) wijkt af van de regeling die in diverse andere wetten zijn opgenomen, waar het gaat om recht op inzage.[99] Daartoe is aanleiding, aangezien de opbouw en structuur van de wijze waarop de persoonsgegevens bij de diensten worden verwerkt – zeker waar het wat oudere gegevens in het (semi)statische archief betreft - een eenvoudige ontsluiting ervan niet altijd mogelijk maakt.[100] Voorts vloeit de langere termijn voort uit het feit dat de beoordeling van de gegevens die wel of niet kunnen worden verstrekt, met het oog op de aard van de gegevens zeer nauw luistert en derhalve meer tijd vergt dan een verzoek op grond van bijvoorbeeld de Wet bescherming persoonsgegevens.

Indien de minister tot het oordeel komt dat de aanvraag kan worden ingewilligd, dan dient deze de aanvrager zo spoedig mogelijk, doch uiterlijk binnen vier weken na bekendmaking van zijn besluit in de gelegenheid te stellen om van zijn gegevens kennis te nemen. In paragraaf 5.4 (artikel 69) is de wijze waarop vervolgens van de gegevens kennis kan worden genomen nader geregeld; daarop zal hieronder nog nader worden ingegaan. Tot slot bepaalt artikel 64, derde lid, dat de betrokken minister zorg dient te dragen voor een deugdelijke vaststelling van de identiteit van de aanvrager; daartoe wordt gevraagd een kopie van een geldig identiteitsbewijs te overleggen.

5.2.3 Kennisneming van persoonsgegevens van een overleden echtgenoot, geregistreerd partner, kind of ouder

Zoals hiervoor is gesteld voorziet de huidige wet, evenals voorliggend wetsvoorstel, erin dat door een beperkte categorie derden ook kennis kan worden genomen van persoonsgegevens, die niet henzelf betreffen. In artikel 67, eerste lid, van het wetsvoorstel (huidig artikel 50, eerste lid), is in verband daarmee bepaald dat artikel 64 van overeenkomstige toepassing is op een aanvraag met betrekking tot persoonsgegevens die zijn verwerkt door of ten behoeve van een dienst ten aanzien van een overleden echtgenoot, geregistreerd partner, kind of ouder van de aanvrager. In artikel 67, tweede lid, worden enkele minimumeisen aan de inhoud van de aanvraag gesteld, waarmee op een zo eenduidig mogelijke manier kan worden vastgesteld op welke overleden persoon de aanvraag betrekking heeft alsmede wat de hoedanigheid van de overledene in relatie tot de aanvrager is. Deze gegevens zijn nodig om niet alleen vast te stellen of de betrokken persoon inderdaad is overleden (aan de hand van een akte van overlijden), maar ook om te beoordelen of de aanvrager inderdaad een beroep op de

[99] In artikel 35, eerste lid, Wet bescherming persoonsgegevens is de termijn gesteld op vier weken; in artikel 25, eerste lid, Wet politiegegevens is de termijn opgesteld op zes weken, waarbij – afhankelijk van de situatie- verdaging mogelijk is met vier dan wel zes weken.
[100] Zie hetgeen daaromtrent onder meer is gesteld in Kamerstukken II 1997/98, 25 877, nr. 3, blz. 64.

kennisnemingregeling kan doen. Is betrokkene inderdaad overleden en behoort de aanvrager tot de kring van personen die tot kennisneming gerechtigd zijn, dan wordt de aanvraag verder in behandeling genomen. In de gevallen dat blijkt dat de aanvraag betrekking heeft op gegevens van een persoon die nog niet is overleden of op gegevens van een overleden persoon die niet de hoedanigheid van echtgenoot, geregistreerd partner, kind of ouder van de aanvrager heeft, dan wordt de aanvraag niet ontvankelijk verklaard (artikel 67, derde lid).

5.2.4 De wijze van kennisneming van gegevens en het afleggen van een verklaring omtrent door de dienst verwerkte gegevens

Indien op grond van artikel 64 door de betrokken minister is besloten dat de aanvrager kennis kan nemen van door of ten behoeve van de dienst verwerkte persoonsgegevens, dan kan dat op verschillende wijzen plaatsvinden. In paragraaf 5.4 (artikel 69) wordt daarvoor een regeling gegeven. Daarbij is voor wat betreft de wijzen waarop de in kennisstelling plaats kan vinden, aangesloten bij artikel 7, eerste lid, van de Wob. Zo bestaan er de volgende mogelijkheden: (a) het geven van een kopie van het document waarin de gegevens zijn neergelegd of door de letterlijke inhoud daarvan in andere vorm te verstrekken, (b) inzage van de inhoud van het document toe te staan, (c) een uittreksel of een samenvatting van de inhoud van het desbetreffende document te geven of (d) inlichtingen uit het desbetreffende document te verschaffen. Anders dan hetgeen in artikel 7, tweede lid, van de Wob is bepaald, is bij de keuze van de wijze van in kennisstelling niet de door de verzoeker (aanvrager) verzochte vorm het uitgangspunt (waarop overigens uitzonderingen mogelijk zijn[101]), maar dient de minister rekening te houden met de voorkeur van de aanvrager en het belang van de dienst. In de praktijk heeft verstrekking van het (bewerkte) document de voorkeur. Tot slot is in artikel 69, derde lid, in de mogelijkheid voorzien dat voor het vervaardigen van kopieën van documenten en uittreksels of samenvattingen van de inhoud daarvan van de aanvrager een vergoeding kan worden gevraagd. Daarop is de op basis van artikel 12 Wob dan wel artikel 14 Wet openbaarheid van bestuur BES vastgestelde regeling ter zake van overeenkomstige toepassing verklaard.

Naar aanleiding van de kennisneming van de omtrent hem door de diensten verwerkte persoonsgegevens, kan de betrokken persoon van oordeel zijn dat de desbetreffende gegevens onjuist of onvolledig zijn dan wel dat deze dienen te worden verwijderd. Bij de totstandkoming van de huidige wet is dan ook expliciet de vraag onder ogen gezien of

[101] Ingevolge artikel 7, tweede lid, van de Wob verstrekt het bestuursorgaan de informatie in de door de verzoeker verzochte vorm, tenzij: (a) het verstrekken van de informatie in die vorm redelijkerwijs niet gevergd kan worden; (b) de informatie reeds in een andere, voor de verzoeker gemakkelijk toegankelijke vorm voor het publiek beschikbaar is.

aan betrokkene ook een recht op verbetering, aanvulling of verwijdering van hem betreffende gegevens zou moeten toekomen (correctierecht). Uiteindelijk is van een dergelijk als zodanig geformuleerd correctierecht om een aantal hierna te memoreren redenen afgezien; ook onderhavig wetsvoorstel voorziet niet in een dergelijk correctierecht. Wel is voorzien in de mogelijkheid dat betrokkene omtrent de gegevens waarvan hij ingevolge artikel 64 kennis heeft genomen, een schriftelijke verklaring kan overleggen, die vervolgens bij diens gegevens wordt gevoegd. Deze voorziening komt, zoals ook in de kabinetsreactie op het rapport van de commissie Dessens ter zake is gesteld, materieel gezien vrijwel geheel overeen met een correctierecht en doet bovendien recht aan de wettelijke plicht tot bronbescherming.[102]

Zoals indertijd ter toelichting op de in artikel 48 Wiv 2002 (het thans voorgestelde artikel 65) is gesteld[103], zou een correctierecht – nu het mede gaat om gegevens die in ieder geval geen operationele waarde meer hebben – in de praktijk slechts een zeer beperkte betekenis kunnen hebben en dan ook alleen voor zover gegevens in het verleden aan anderen zijn verstrekt en desbetreffende gegevens nog door hen zouden (kunnen) worden gebruikt. Een bijkomend probleem bij het toekennen van een correctierecht is dat in een discussie over de vraag of een gegeven correct is, de dienst veelal niet ten volle daaraan kan deelnemen zonder de bronnen te onthullen waaruit het desbetreffende gegeven afkomstig is. De dienst zou daarmee in een onmogelijke bewijspositie worden gedrongen. Door te voorzien in de mogelijkheid dat betrokkene een verklaring kan afleggen over bijvoorbeeld gegevens waarvan hij meent dat die onjuist of onvolledig zijn en die te doen opnemen in zijn dossier, wordt zowel het belang van betrokkene als dat van de dienst op een evenwichtige wijze gediend. Daarbij komt dat, indien de desbetreffende gegevens op grond van artikel 55, tweede lid, van het wetsvoorstel toch nog worden verstrekt, ingevolge het bepaalde in artikel 55, derde lid, van het wetsvoorstel een aanwezige verklaring die op de desbetreffende gegevens betrekking heeft, gelijktijdig dient te worden verstrekt. Op deze wijze wordt de persoon of instantie aan wie de gegevens worden verstrekt ook van de zienswijze van de betrokkene ter zake op de hoogte gesteld (zie huidig artikel 41 Wiv 2002).

Het voorgaande laat natuurlijk onverlet dat, indien de diensten zelf tot de bevinding komen dat een gegeven onjuist is of ten onrechte wordt verwerkt, zij verplicht zijn dat gegeven te verbeteren onderscheidenlijk te verwijderen (zie artikel 57 van het wetsvoorstel).

[102] Kamerstukken II 2013/14, 33 820, nr. 2, blz. 7-8.
[103] Zie Kamerstukken II 1997/98, 25 877, nr. 3, blz. 66-67.

5.2.5 Kennisneming van eigen persoonsgegevens door (oud)medewerkers van de diensten

Het wetsvoorstel voorziet, evenals nu, in een van artikel 64 afwijkende regeling met betrekking tot kennisneming van persoonsgegevens door personen die werkzaam zijn (geweest) bij of ten behoeve van een dienst, waar het gaat om kennisneming van gegevens die omtrent hen zijn opgenomen in de personeels- en salarisadministratie van de dienst; ook wordt voorzien in de mogelijkheid tot verbetering van de verwerkte gegevens. Het is immers evident dat de regeling in de artikelen 64 en 67 die in algemene zin geldt voor kennisneming van persoonsgegevens die door de diensten zijn verwerkt in het kader van de uitvoering van de wet op de inlichtingen- en veiligheidsdiensten of de Wvo, voor zover het gaat om personen die – over het algemeen als ambtenaar – werkzaam zijn of zijn geweest voor één van de diensten niet van toepassing kan zijn. Tussen laatstgenoemde personen en de diensten bestaat (of bestond) immers een "werkgever-werknemer"-verhouding.[104] Van de in dat kader verwerkte gegevens moet door de betrokken persoon kennis kunnen worden genomen en indien daartoe aanleiding bestaat moeten hem betreffende gegevens kunnen worden verbeterd.

In artikel 66, eerste lid, is in verband hiermee bepaald, dat het hoofd van een dienst een persoon werkzaam bij of ten behoeve van een dienst of werkzaam geweest bij of ten behoeve van een dienst, op diens verzoek zo spoedig mogelijk, doch uiterlijk binnen vier weken na het verzoek, in de gelegenheid stelt om van zijn gegevens in de personeels- en salarisadministratie van de desbetreffende dienst kennis te kunnen nemen. Dit recht vloeit rechtstreeks voort uit de wet en vergt dus geen afzonderlijk besluit van de betrokken minister. Ingevolge artikel 66, tweede lid, zijn van inzage uitgezonderd de gegevens die zicht kunnen geven op bronnen die geheim moeten worden gehouden. Zoals eerder al in deze memorie van toelichting is aangegeven, is bronbescherming één van de belangrijkste principes in het werk van inlichtingen- en veiligheidsdiensten. In het kader van de toepassing van onderhavige bepaling gaat het om de bescherming van de identiteit van bronnen die gegevens hebben verstrekt, bijvoorbeeld in het kader van een veiligheidsonderzoek. In het derde lid is bepaald dat het hoofd van de dienst, in afwijking van het bepaalde in artikel 2:1, eerste lid, Awb, kan bepalen dat kennisneming van de gegevens slechts is voorbehouden aan de betrokken persoon persoonlijk. In artikel 2:1, eerste lid, Awb, is bepaald, dat een ieder ter behartiging van zijn belangen in het verkeer met bestuursorganen zich kan laten bijstaan of door een gemachtigde kan laten

[104] Waar het gaat om de ambtenaren, bedoeld in de artikelen 79 en 80, bestaat er geen reguliere werkgever-werknemer relatie met de dienst waarvoor zij werkzaamheden verrichten, aangezien zij in dienst zijn van andere organisaties. Niettemin worden omtrent hen bij de diensten gegevens verwerkt die deels vergelijkbaar zijn met de gegevens die door de diensten worden verwerkt omtrent de medewerkers die wel bij hen in dienst zijn.

vertegenwoordigen. Het kan voor komen dat bepaalde gegevens zodanig gevoelig zijn, bijvoorbeeld operationele gegevens betreffende de aangenomen identiteit van betrokkene, dat de kennisneming daarvan uitsluitend tot de betrokken persoon persoonlijk dient te worden beperkt. Artikel 66, derde lid, biedt daartoe aldus de mogelijkheid. Tegen dit besluit staat bezwaar en beroep open. Anders dan bij inzage op grond van artikel 64 of artikel 67 komt aan de betrokkene met betrekking tot de omtrent hem opgenomen gegevens in de personeels- en salarisadministratie wel een recht op verbetering toe. Ingevolge het vierde lid kan degene die inzage heeft gehad van de hem betreffende gegevens het hoofd van de dienst schriftelijk verzoeken om deze te verbeteren, aan te vullen of te verwijderen, indien deze feitelijk onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn dan wel in strijd met een wettelijk voorschrift zijn verwerkt. In het verzoek dient aangegeven worden welke wijzigingen er aangebracht zouden moeten worden. Het hoofd van de betreffende dienst dient vervolgens binnen zes weken na ontvangst van het verzoek aan betrokkene mede te delen of en, zo ja, in hoeverre aan het verzoek wordt voldaan. Deze mededeling is een besluit in de zin van de Awb. Tot slot is in artikel 66, zesde lid, artikel 73 niet van toepassing verklaard. Dat artikel ziet op de mogelijkheid om gegevens over persoonlijke beleidsopvattingen bij een verzoek om inzage te weigeren; dat is dus hier niet mogelijk.

5.3 Het recht op kennisneming van andere gegevens dan persoonsgegevens

In paragraaf 5.3 (artikel 68) van het wetsvoorstel is het recht op kennisneming van andere gegevens dan persoonsgegevens opgenomen. Op grond van artikel 68, eerste lid, deelt de betrokken minister een ieder op diens aanvraag zo spoedig mogelijk, doch uiterlijk binnen drie maanden mede of kennis kan worden genomen van andere dan persoonsgegevens betreffende de in de aanvraag vermelde bestuurlijke aangelegenheid. Ingevolge artikel 63 wordt onder bestuurlijke aangelegenheid hier hetzelfde verstaan als in de Wob en in de Wet openbaarheid van bestuur BES.

In procedureel opzicht sluit deze regeling aan bij hetgeen is geregeld voor het kennisnemen van persoonsgegevens. Dat geldt niet alleen voor de beslistermijn en – bij een positief besluit – de termijn waarbinnen de aanvrager in staat dient te worden gesteld om van de gegevens kennis te nemen, maar evenzeer voor de wijze waarop die in kennisstelling kan plaatsvinden.

Hetgeen eerder in deze memorie van toelichting is gesteld omtrent de beslistermijn, geldt mutatis mutandis ook hier. Niet alleen zullen gegevens die betrekking hebben op een bestuurlijke aangelegenheid dienen te worden gecontroleerd op de aanwezigheid van persoonsgegevens, maar vervolgens zullen de gevonden gegevens dienen te worden beoordeeld in het licht van de weigeringsgronden (zie hierna) en voor zover noodzakelijk

te worden gescreend. Een termijn van drie maanden (met de mogelijkheid tot verlenging met een periode van vier weken) is dan ook bij de beoordeling van dit soort aanvragen veelal noodzakelijk.

5.4 Weigeringsgronden en beperkingen

In paragraaf 5.5 (de artikelen 70 tot en met 73) van het wetsvoorstel worden de weigeringsgronden en beperkingen geregeld, die bij de beoordeling van een verzoek om kennisneming van persoonsgegevens onderscheidenlijk andere gegevens dan persoonsgegevens dienen te worden gehanteerd. Ook dit toetsingskader is ongewijzigd uit de huidige wet (de artikelen 53 tot en met 56) overgenomen; bij de totstandkoming daarvan is uitvoerig stilgestaan bij de overwegingen die aan de daarbij gemaakte keuzes, met name waarom niet volstaan kon worden met het overnemen van de weigeringsgronden uit de Wob, maar dat waar het gaat om kennisneming van (eigen) persoonsgegevens een aantal specifieke weigeringsgronden dienen te gelden. [105]

Daarbij is allereerst in meer algemene zin opgemerkt, dat de diensten hun wettelijke taken uitsluitend binnen een zekere mate van geheimhouding effectief kunnen uitvoeren, waarbij een drietal criteria een rol spelen. Bronnen, werkwijzen ("*modus operandi*") en actueel kennisniveau dienen geheim te kunnen worden gehouden. Dat zijn de zogeheten kritische ondergrenzen, die als een vertaling kunnen worden gezien van het zgn. "jeopardize"- criterium uit de jurisprudentie van het EHRM.[106] Dit criterium houdt in dat de lange-termijndoeleinden die tot het onderzoek aanleiding gaven, niet in gevaar mogen komen. Overschrijding van deze kritische ondergrenzen betekent dat dit het goed functioneren van de diensten aantast en daarmee – uiteindelijk - ook de nationale veiligheid. Daarbij is aangegeven dat met name het criterium "actueel kennisniveau" bij de beoordeling van een inzageverzoek in persoonsgegevens van doorslaggevende betekenis is.[107] Daarbij gaat het om bij de diensten aanwezige kennis omtrent actuele bedreigingen van de nationale veiligheid. Indien die kennis bekend zou raken, kan dat door betrokkene gebruikt worden om (de lange-termijndoeleinden van de) onderzoeken van de diensten te frustreren. De conclusie die daaruit is getrokken en uiteindelijk ook zijn wettelijke vertaling heeft gekregen is dat een inzageverzoek alleen kan worden ingewilligd, indien deze uitdrukkelijk wordt beperkt tot kennisneming van niet-actuele persoonsgegevens. Dat betreffen persoonsgegevens die omtrent de aanvrager zijn verwerkt door de diensten, maar waarvan de wetenschap daarover voor de huidige taakuitvoering van de diensten niet langer meer relevant is. Dergelijke gegevens kunnen

[105] Zie onder meer Kamerstukken II 1997/98, 25 877, nr. 3, blz. 68-71.
[106] Zie *Klass e.a. t. Duitsland*, par. 58.
[107] Kamerstukken II 1997/98, 25 877, nr. 3, blz. 69.

in beginsel worden verstrekt, zij het dat natuurlijk ook nog getoetst zal moeten worden aan de andere van toepassing zijnde weigeringsgronden.

Een en ander heeft ertoe geleid dat waar het gaat om kennisneming van (eigen) persoonsgegevens een specifieke weigeringsgrond is geformuleerd[108], die thans in artikel 70 van het wetsvoorstel (huidig artikel 53 Wiv 2020) is neergelegd. Met deze weigeringsgrond wordt het toetsingscriterium "actueel kennisniveau" op wetsniveau nader uitgewerkt. Nu artikel 70 in het kader van de kennisneming van persoonsgegevens voor dit toetsingscriterium een uitputtende regeling geeft, kan daarvoor dan ook geen beroep meer worden gedaan op de in artikel 72, eerste lid, neergelegde (absolute) weigeringsgrond "nationale veiligheid".

Het begrip "actueel kennisniveau" heeft een tweetal componenten: de component dat er omtrent de betrokken persoon actuele gegevens bij de diensten aanwezig zijn en de component dat er in het geheel geen gegevens aanwezig zijn. Zowel het eerste als het tweede gegeven kunnen ertoe leiden dat als dat bij de betrokken persoon bekend raakt, hij lopende onderzoeken van de diensten kan frustreren door zijn gedrag op die kennis af te stemmen.[109] In beide gevallen dient dus een weigering van het verzoek mogelijk te zijn.

In artikel 70 van het wetsvoorstel is dit – in navolging van artikel 53 van de Wiv 2002 – als volgt uitgewerkt. Een aanvraag als bedoeld in artikel 64 wordt in ieder geval afgewezen, indien:

a. betreffende de aanvrager in het kader van enig onderzoek gegevens zijn verwerkt, tenzij:

> 1°.de desbetreffende gegevens meer dan 5 jaar geleden zijn verwerkt,
> 2°. met betrekking tot de aanvrager sindsdien geen nieuwe gegevens zijn verwerkt, en
> 3°. de desbetreffende gegevens niet relevant zijn voor enig lopend onderzoek;

b. betreffende de aanvrager geen gegevens zijn verwerkt.

In deze (bestaande) regeling wordt dus in het eerste lid, onderdeel a, onder 1°, als uitgangspunt gehanteerd dat gegevens die minder dan vijf jaar geleden zijn verwerkt altijd als actueel moeten worden aangemerkt en nimmer zullen worden verstrekt; dit uitgangspunt heeft als bijkomend voordeel dat de bestuurlijke lasten voor de behandeling

[108] Artikel 71 verklaart artikel 70 van overeenkomstige toepassing op een aanvraag als bedoeld in artikel 67.
[109] Zie ook Kamerstukken II 2000/01, 25 877, nr. 14, blz. 75.

van verzoeken om kennisneming aanzienlijk worden verminderd. Vanwege de samenhang tussen notificatie (het uitbrengen van een verslag dat jegens betrokkene een bijzondere bevoegdheid is ingezet) en de kennisnemingsregeling (een notificatie kan immers leiden tot een verzoek om kennisneming van de bij de dienst omtrent betrokkene verwerkte gegevens) wordt ook in de notificatieregeling een termijn van vijf jaar gehanteerd, waarna de onderzoeksverplichting ter zake ontstaat.

Het in het eerste lid, onderdeel a, onder 2°, neergelegde criterium brengt de gedachte tot uitdrukking dat in de situatie dat gegevens minder dan vijf jaar geleden zijn verwerkt in het kader van één en hetzelfde onderzoek waarvan ook gegevens meer dan vijf jaar geleden zijn verwerkt, dat onderzoek en daarmee ook de gegevens – ongeacht of zij nu meer of minder dan vijf jaar geleden zijn verwerkt – nog actueel zijn.[110]

Het derde criterium – eerste lid, onderdeel a, onder 3° – brengt tot uitdrukking dat de gegevens niet meer relevant mogen zijn voor enig lopend onderzoek. Bij de toepassing van dit onderdeel is met name de uitleg van het begrip "lopend onderzoek" van cruciaal belang.

De tweede, hiervoor genoemde, component van het begrip "actueel kennisniveau" heeft in artikel 70, eerste lid, onderdeel b, zijn uitwerking gekregen. Ingevolge artikel 70, tweede lid, dient ingeval dat een aanvraag op grond van het eerste lid moet worden afgewezen, bij de motivering van de afwijzing slechts in algemene termen te worden gewezen op alle aldaar vermelde gronden voor de afwijzing. Aldus wordt bewerkstelligd dat in het midden wordt gelaten of er nu wel of niet actuele gegevens of in het geheel geen gegevens omtrent betrokkene door de dienst wordt verwerkt.

In artikel 71 is de regeling van artikel 70 ook van toepassing verklaard op verzoeken om kennisneming van door of ten behoeve van de diensten verwerkte persoonsgegevens als bedoeld in artikel 67 van het wetsvoorstel.

In artikel 72, eerste en tweede lid, van het wetsvoorstel zijn de weigeringsgronden opgenomen die van toepassing zijn bij de beoordeling van een aanvraag als bedoeld in artikel 68 (kennisneming van andere gegevens dan persoonsgegevens), alsmede bij de (verdere) beoordeling van een verzoek om kennisneming van persoonsgegevens, voor zover een dergelijke aanvraag niet wordt afgewezen op grond van artikel 70 of 71 (artikel 72, vierde lid). De hier opgenomen weigeringsgronden komen vrijwel geheel

[110] Zie Kamerstukken II 1997/98, 25 877, A, blz. 9.

overeen met de weigeringsgronden in artikel 10, eerste en tweede lid, Wob.[111] Van een verdere toelichting ter zake wordt hier daarom ook afgezien.

Mocht de beoordeling van het verzoek om kennisneming ertoe leiden dat deze dient te worden afgewezen, dan moet ingevolge artikel 72, derde lid, de CTIVD daarvan gemotiveerd op de hoogte worden gesteld; dit geldt niet alleen in geval dat het gaat om een aanvraag als bedoeld in artikel 68, maar ingevolge artikel 72, vierde lid, ook voor aanvragen als bedoeld in artikel 64 onderscheidenlijk 67. De CTIVD kan vervolgens in het kader van haar taak om toe te zien op de rechtmatige uitvoering van deze wet beoordelen of de weigering aan de wettelijke eisen voldoet.

In artikel 73 is ten slotte een regeling opgenomen inzake de verstrekking van persoonlijke beleidsopvattingen, die zijn opgenomen in documenten opgesteld ten behoeve van intern beraad. Deze regeling komt overeen met het bepaalde in artikel 11, eerste tot en met derde lid, Wob en behoeft geen verdere toelichting.

Hoofdstuk 6 Samenwerking tussen inlichtingen- en veiligheidsdiensten en met andere instanties

6.1 Algemeen

In hoofdstuk 6 van het wetsvoorstel worden regels gegeven voor de samenwerking tussen de AIVD en MIVD, de samenwerking van deze diensten met inlichtingen- en veiligheidsdiensten van andere landen en de samenwerking met andere instanties, zoals de politie, het openbaar ministerie, de rijksbelastingdienst, de Immigratie en Naturalisatiedienst (IND) en de KMar. Voorts wordt bepaald dat bij of krachtens algemene maatregel van bestuur nadere regels gesteld kunnen worden met betrekking tot door de diensten in het kader van een goede taakuitvoering met een of meer instanties aangegane samenwerkingsverbanden. De in het wetsvoorstel opgenomen regeling is ten opzichte van de bestaande regeling in hoofdstuk 5 van de Wiv 2002 op onderdelen aangevuld en nader uitgewerkt. In het onderstaande wordt een en ander nader toegelicht.

6.2 De samenwerking tussen Algemene Inlichtingen- en Veiligheidsdienst en Militaire Inlichtingen- en Veiligheidsdienst

In de artikelen 74 en 75 wordt het wettelijk kader gegeven voor de samenwerking tussen de AIVD en de MIVD. Artikel 74 sluit aan bij hetgeen thans in artikel 58 van de huidige wet is geregeld, zij het dat overeenkomstig de aanbeveling van de commissie Dessens de

[111] Het begrip veiligheid van de staat is in artikel 72, eerste lid, onder b, vervangen door nationale veiligheid; zie ook het huidige artikel 55, eerste lid, onder b, Wiv 2002.

regeling van samenwerking tussen de diensten verder gaat dan de huidige plicht om elkaar zoveel mogelijk medewerking te *verlenen* en aan de diensten opdraagt om zoveel mogelijk *samen te werken* (artikel 74, eerste lid). Daarmee wordt ook uitdrukking gegeven aan een ontwikkeling in de afgelopen jaren, waarbij in toenemende mate in gezamenlijk werkverbanden (gemeenschappelijk teams) en op operationeel gebied wordt samengewerkt. Met het nieuwe artikel 74, vierde lid, waarop hierna nog afzonderlijk wordt ingegaan, wordt beoogd dat proces te faciliteren.

Artikel 74, tweede lid, van het wetsvoorstel omschrijft – evenals het huidige artikel 58, tweede lid - waaruit die samenwerking in ieder geval kan bestaan, namelijk (a) de verstrekking van gegevens en (b) het verlenen van technische en andere vormen van ondersteuning. In artikel 74, derde lid, is de procedure die bij verzoeken om technische en andere vormen van ondersteuning moet worden gevolgd voor zover deze betrekking hebben op de uitoefening van bijzondere bevoegdheden als bedoeld in paragraaf 3.3.2 (gericht op gegevensverwerking), 4.2 of 4.3 (overige bijzondere bevoegdheden) uitgewerkt. Daarin is ten opzichte van de huidige situatie geen wijziging aangebracht. Een verzoek tot ondersteuning wordt gedaan door de voor de verzoekende dienst verantwoordelijke minister en omvat een nauwkeurige omschrijving van de verlangde werkzaamheden. Voorts wordt in het derde lid bepaald, dat de minister die om de medewerking heeft verzocht, verantwoordelijk is voor de feitelijke uitvoering van de te verrichten werkzaamheden. Dat daarbij ambtenaren van een dienst worden ingeschakeld die onder de verantwoordelijkheid van een andere minister vallen, doet daar niet aan af.

De commissie Dessens is van mening dat de wet ruimte moet gaan bieden aan verdergaande samenwerkingsvormen dan waar artikel 58 van de huidige wet het kader voor biedt. Volgens de commissie maakt de huidige regeling het niet makkelijk om een gezamenlijke organisatie op te richten die de uitvoering van een taak voor beide diensten op zich kan nemen, bijvoorbeeld als het gaat om de wijze waarop de sturing van een intensief samenwerkingsverband als de Joint Sigint Cyber Unit (JSCU) moet worden vormgegeven en waarbij ook de feitelijke uitvoering van de uitoefening van bijzondere bevoegdheden bij het samenwerkingsverband wordt belegd. Met het voorgestelde artikel 74, vierde lid, wordt beoogd hiervoor de nodige ruimte te bieden, echter zonder dat de bestaande verantwoordelijkheidsverdeling wordt aangetast. Immers te allen tijde moet duidelijk zijn welke minister voor welke handeling van het desbetreffende samenwerkingsverband verantwoordelijk en aanspreekbaar is. Indien de behoefte bestaat om daarin wijziging aan te brengen, zal dat op formeelwettelijk niveau dienen plaats te vinden. Daartoe bestaat echter thans geen voornemen.

Op grond van artikel 74, vierde lid, kunnen de ministers met betrekking tot een gezamenlijk werkverband van de diensten bij ministeriële regeling nadere regels stellen. Op dit moment worden ter zake tussen de ministers bestuursafspraken (neergelegd in een "convenant") gemaakt.[112] Met de in het vierde lid voorgestelde regeling wordt aan dergelijke samenwerkingsverbanden een expliciete wettelijke grondslag gegeven, dat ook deel uit gaat maken van het wettelijk kader waarover het rechtmatigheidstoezicht van de CTIVD zich uitstrekt. Overigens wordt opgemerkt dat ook bij dergelijke regelingen voorzien kan zijn in een geheim deel, bijvoorbeeld wanneer dit deel zicht zou geven op het actueel kennisniveau van de diensten, de bronnen en de gehanteerde werkwijzen (*modus operandi*). In de hiervoor genoemde convenanten kunnen afspraken zijn neergelegd die betrekking hebben op de uitwisseling van gegevens tussen de diensten. In een dergelijk convenant kunnen echter ook afspraken worden gemaakt over de ondersteuning bij de uitoefening van bijzondere bevoegdheden, waarbij echter niet afgeweken kan worden van het bepaalde in artikel 58, derde lid, van de huidige wet. Dat betekent dat in samenwerkingsverbanden in de gevallen dat bij de uitoefening van een bijzondere bevoegdheid technische of andere vormen van ondersteuning nodig is, het kan voorkomen dat men toch iedere keer een afzonderlijk verzoek daartoe moet doen. Dat is niet altijd efficiënt. In het voorgestelde vierde lid wordt ter zake bepaald dat als de ministeriële regeling betrekking heeft op de *ondersteuning* bij de toepassing van een bijzondere bevoegdheid, het bepaalde in derde lid, eerste volzin, ter zake buiten toepassing blijft. Dat neemt niet weg dat in de regeling een nauwkeurige omschrijving dient te worden opgenomen van de desbetreffende ondersteuning; voorts blijft de in het derde lid opgenomen verantwoordelijkheidsverdeling onverlet.

Tot slot is in artikel 74, vijfde lid, een voorziening opgenomen voor het geval dat het verzoek om ondersteuning louter bestaat uit het ter beschikking stellen van technische apparatuur (zoals bijvoorbeeld een IMSI-catcher). In dat geval kan het verzoek ook door of namens het hoofd van de betrokken dienst worden gedaan.

Artikel 75 van het wetsvoorstel biedt ten opzichte van de huidige wet een nieuwe regeling, waarbij, onder verwijzing naar de samenwerking in artikel 74, eerste lid, aan de AIVD onderscheidenlijk de MIVD de zorgplicht wordt opgedragen om de andere dienst tijdig te informeren over voorgenomen operationele activiteiten in Nederland en in andere landen, die naar verwachting van invloed kunnen zijn op een goede taakuitvoering van die andere dienst ('need to share'). Deze nieuwe bepaling reflecteert de aanpassing aan de eisen die heden ten dage aan de samenwerking tussen beide diensten moeten worden gesteld, namelijk een intensieve taakoverstijgende

[112] Vergelijk het convenant JSCU; bijlage bij Kamerstukken II 2013/14, 29 924, nr. 113.

samenwerking, waarbij afstemming 'aan de voorkant' centraal staat. De bestaande deconflictieregeling, zoals die bij verschillende bijzondere bevoegdheden is opgenomen, en waarbij – kort gezegd - de MIVD voor de uitoefening van bijzondere bevoegdheden "buiten plaatsen in gebruik van het Ministerie van Defensie" (ook wel: het civiele domein) overeenstemming met de AIVD dient te bereiken, komt met artikel 75 te vervallen.[113] Er wordt daarmee voor een andere, meer bij de intensievere samenwerking aansluitende benadering gekozen. Maximale onderlinge voorafgaande afstemming staat daarbij voorop. Dat kan er ook toe bijdragen dat de diensten de hun beschikbare middelen op een efficiëntere wijze inzetten; indien bij een dergelijke afstemming blijkt dat een dienst reeds een bepaalde inzet uitvoert en de andere dienst dat ook wil doen, dan kan nadrukkelijk bezien worden of die inzet niet tevens voor de andere dienst kan plaatsvinden. Met deze regeling wordt bovendien aangesloten bij de nieuwe Geïntegreerde Aanwijzing, die zowel de inlichtingen- als veiligheidstaak, alsook het binnen- en buitenlandse werkterrein van beide diensten behelst en waarbij op hoofdlijnen inzicht wordt gegeven in elkaars operationele mogelijkheden en (geplande) inzet. In het tweede lid van artikel 75 is een regeling getroffen voor de uitzonderlijke situatie waarin de eigen taakuitvoering van een dienst zich verzet tegen het verstrekken van informatie als bedoeld in het eerste lid van artikel 75. In een dergelijk geval treden de hoofden van de diensten met elkaar in overleg. Deze bepaling is bedoeld voor uitzonderlijke gevallen waarbij bijvoorbeeld de bronbescherming van agenten in zeer gevoelige operaties met zich meebrengt dat de afstemming enkel op diensthoofdenniveau onderwerp van gesprek kan zijn.

6.3 Samenwerking met inlichtingen- en veiligheidsdiensten van andere landen

6.3.1 Algemeen

De AIVD en de MIVD werken sinds jaar en dag met een veelheid van buitenlandse diensten samen. Deze samenwerking heeft door de internationale ontwikkelingen op veiligheidsgebied, vergelijk de situatie in het Midden Oosten en Noord-Afrika, alleen maar aan belang en intensiteit gewonnen. In de jaarverslagen van beide diensten in de afgelopen jaren is daar regelmatig bij stilgestaan. Samenwerking met buitenlandse diensten is ook van belang, omdat op deze wijze voor de nationale veiligheid van Nederland belangrijke informatie kan worden verkregen. In het metier van inlichtingen- en veiligheidsdiensten is immers bij de uitwisseling van informatie het beginsel van 'quid pro quo' (voor wat hoort wat) een belangrijk element; zonder wederkerigheid, geen informatie. Ook de CTIVD heeft in een aantal toezichtsrapporten aandacht besteed aan

[113] Zie de artikelen 20, tweede lid, 22, tweede en vierde lid, 23, derde lid, 24, tweede lid, 25, derde en vijfde lid, 27, achtste lid, en 28, vijfde lid, Wiv 2002.

(diverse aspecten van) de samenwerking van de AIVD met buitenlandse collega-diensten[114]; een vervolgonderzoek naar de samenwerking van de AIVD met buitenlandse inlichtingen- en veiligheidsdiensten alsmede een onderzoek naar de samenwerking van de MIVD met buitenlandse collega-diensten vindt thans plaats. In artikel 59 van de huidige wet is voor die samenwerking een kader opgenomen. Dit kader is aan heroverweging en verdere uitbouw toe. Zowel de rapporten van de CTIVD als de aanbevelingen van de commissie Dessens ter zake, alsmede hetgeen met in het bijzonder de Tweede Kamer in dit verband is gewisseld, nopen daartoe.

In paragraaf 6.2 van het wetsvoorstel is het (deels) nieuwe kader voor samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten opgenomen. Deze valt uiteen in een drietal onderdelen. Allereerst wordt in artikel 76 de bevoegdheid tot het aangaan van samenwerkingsrelaties met buitenlandse collega-diensten geregeld alsmede de daaraan voorafgaand door de diensten te maken weging die bepalend is voor de vraag of en, zo ja, waaruit die samenwerking kan bestaan. In artikel 77 wordt een regeling gegeven voor de verstrekking van gegevens alsmede het verlenen van technische en andere vormen van ondersteuning *aan* buitenlandse collega-diensten. Artikel 78 geeft tot slot een regeling voor het doen van verzoeken om technische en andere vormen van ondersteuning aan buitenlandse collega-diensten *door* de AIVD of MIVD. Een regeling voor dit laatste ontbreekt in de huidige wet.

6.3.2 Het aangaan van en onderhouden van samenwerkingsrelaties met inlichtingen- en veiligheidsdiensten van andere landen

Artikel 59, eerste lid, van de Wiv 2002 legt aan de hoofden van de diensten de zorgplicht op om verbindingen te onderhouden met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen. Daarbij geldt als uitgangspunt dat de AIVD de contacten onderhoudt met de civiele inlichtingen- en veiligheidsdiensten en de MIVD de contacten met de militaire inlichtingen- en veiligheidsdiensten. Met de totstandkoming van de Joint Sigint en Cyber Unit treedt het hoofd van deze gemeenschappelijk eenheid als POC (point of contact) op voor het – namens de beide diensthoofden – onderhouden van de contacten met de internationale Sigint-gemeenschap.

De beoordeling met welke diensten van welke landen wordt samengewerkt wordt thans op het niveau van – het hoofd van - de dienst zelf gemaakt, hetgeen overigens niet betekent dat er geen afstemming met de politiek verantwoordelijke bewindspersoon

[114] Vergelijk onder meer CTIVD-rapport nr. 22a (2009) inzake de samenwerking van de AIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, rapport nr. 26 (2011) inzake de uitvoering van de inlichtingentaak door de AIVD, rapport nr. 28 (2011) inzake de inzet van Sigint door de MIVD. Maar ook het recente rapport nr. 38 inzake de gegevensverwerking van de AIVD en MIVD op het gebied van telecommunicatie gaat in op de samenwerking ter zake met buitenlandse diensten.

plaatsvindt. De betrokken minister dient over de samenwerking te worden geïnformeerd en bij risicovolle collega-diensten dient de besluitvorming aan de minister te worden voorgelegd.[115] Voorafgaand aan het aangaan van een samenwerkingsrelatie met een buitenlandse inlichtingen- of veiligheidsdienst worden een aantal zaken onderzocht.[116] Bezien wordt hoe het is gesteld met de democratische inbedding, de taken, de professionaliteit en de betrouwbaarheid van de dienst. Verder wordt onderzocht of internationale verplichtingen[117] samenwerking wenselijk maken en in hoeverre de samenwerking met de buitenlandse dienst de goede taakuitvoering door de Nederlandse diensten kan bevorderen. Deze factoren worden in onderling verband gewogen. Ook de CTIVD refereert in rapport 22a (2009) aan deze alsmede enkele andere criteria.[118] De commissie Dessens heeft in haar rapport opgemerkt dat de hier beschreven criteria niet in de wet zijn opgenomen. De commissie Dessens vindt dat het wettelijk kader in artikel 59 Wiv 2002 heroverweging verdient en dat, mede in het licht van de discussies over de NSA, nader onderzocht moet worden of de Wiv voor de samenwerking met buitenlandse diensten voldoende rechtsstatelijke en democratische garanties bevat. In reactie op deze aanbeveling van de commissie is door het kabinet aangegeven dat wereldwijde internationale samenwerking voor de inlichtingen- en veiligheidsdiensten een *conditio sine qua non* is. De aard en de intensiteit van die samenwerking moet mede worden bepaald door criteria als de democratische inbedding van de desbetreffende dienst, het mensenrechtenbeleid van het desbetreffende land, de professionaliteit en betrouwbaarheid en het karakter van de dienst. De wet moet daarvoor voldoende kader en ruimte bieden.

De CTIVD heeft in rapport 38 (februari 2014) opgemerkt dat het aan de hoofden van de AIVD en de MIVD onder de politieke verantwoordelijkheid van de betrokken minister te overwegen is of buitenlandse diensten nog steeds in aanmerking komen voor de verschillende vormen van samenwerking die plaatsvinden in het kader van de hechte samenwerkingsrelatie. Daarbij zouden ook de wettelijke bevoegdheden en (technische) mogelijkheden van buitenlandse diensten dienen te worden betrokken. Samenwerkingsrelaties (ook op internationaal niveau) dienen te worden beoordeeld op transparantie en de afwegingen die ten grondslag liggen aan de samenwerking zouden

---

[116] Kamerstukken II 2000/01, 25 877, nr. 59, p. 16 en Aanhangsel Handelingen II 2004/05, nr. 749.

[117] Zo is Nederland partij bij verdragen op het vlak terrorismebestrijding, hetgeen tot samenwerkig – ook tussen inlichtingen- en veiligheidsdiensten – noopt.

[118] De CTIVD noemt zelf de volgende criteria: het respect voor de mensenrechten, de democratische inbedding, de taken, de professionaliteit en de betrouwbaarheid van de dienst, de wenselijkheid van de samenwerking in het kader van internationale verplichtingen, de bevordering van de taakuitvoering en de mate van wederkerigheid ('quid pro quo').

nader moeten worden geconcretiseerd. De betrokken ministers hebben in hun reactie aangegeven dat de aanbeveling wordt opgevolgd.

In het voorgestelde artikel 76 wordt uitvoering gegeven aan het door het kabinet ingenomen standpunt ten aanzien van de aanbevelingen van de commissie Dessens en de CTIVD.

Het voorgestelde artikel 76, eerste lid, geeft – evenals het huidige artikel 59, eerste lid, van de wet - de algemene bevoegdheid aan de AIVD en MIVD om samenwerkingsrelaties aan te gaan met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen. In het tweede lid wordt bepaald dat de AIVD en MIVD voorafgaand aan het aangaan van een samenwerkingsrelatie een weging maken aan de hand van de criteria als bedoeld in het derde lid of kan worden overgegaan tot het aangaan van een samenwerkingsrelatie en, zo ja, wat de aard en intensiteit van de beoogde samenwerking kan zijn. De daarbij toe te passen criteria betreffen in ieder geval: de democratische inbedding van de dienst in het desbetreffende land, de eerbiediging van de mensenrechten door het desbetreffende land en de professionaliteit en betrouwbaarheid van de desbetreffende dienst.

Voor het kunnen maken van de hier bedoelde weging is het nodig de daarvoor benodigde informatie te verkrijgen. Daarbij kan door de diensten gebruik gemaakt worden van informatie uit open bronnen of uit de signalen die zij hebben verkregen vanuit eerdere samenwerking of vanuit de bredere internationale inlichtingengemeenschap. Of een dienst in voldoende mate democratisch is ingebed, hangt af van een aantal factoren. Zo kan onder meer worden gekeken naar het algehele politieke bestel van het land in kwestie en de positie die de desbetreffende dienst daarin inneemt, de wettelijke bevoegdheden van de dienst en het (onafhankelijke) toezicht daarop. Met betrekking tot het criterium respect voor de mensenrechten, kan bijvoorbeeld bezien worden of het desbetreffende land internationale mensenrechtenverdragen heeft geratificeerd en of deze mensenrechtenverdragen in de praktijk nageleefd worden. Eveneens is het van belang of een buitenlandse collega-dienst in verband wordt of is gebracht met schendingen van mensenrechten. Zo kan, bijvoorbeeld, worden gekeken naar signaleringen van schendingen van mensenrechten in onderzoeken en rapporten van nationale en internationale mensenrechtenorganisaties. Daarnaast is de mate waarin een buitenlandse collega-dienst als professioneel en als betrouwbaar kan worden beschouwd grotendeels afhankelijk van de ervaringen van de AIVD en MIVD die zijn opgedaan in de samenwerkingsrelatie met de betrokken dienst. Tevens worden met andere (bevriende) collega-diensten opvattingen en ervaringen in dit kader uitgewisseld, wat kan bijdragen aan de inschatting of een buitenlandse dienst professioneel en betrouwbaar is. De

professionaliteit en betrouwbaarheid van een collega-dienst zijn voorts belangrijke factoren bij de besluitvorming omtrent een eventuele intensivering van de samenwerkingsrelatie. Ook het door de CTIVD in rapport 38 opgebrachte criterium inzake transparantie is daarin uitgewerkt. In het kader van transparantie wordt beoordeeld in hoeverre buitenlandse diensten inzicht geven in hun taken, bevoegdheden en werkwijze. Het betreft daarmee een methodiek om vast te stellen in hoeverre andere diensten democratisch zijn ingebed en mensenrechten respecteren. De weging van deze criteria is dus afhankelijk van de mate waarin hierover transparantie bestaat; onvoldoende transparantie is dus een sterke contra-indicatie voor samenwerking.

Het resultaat van de weging moet antwoord geven op de vraag of en, zo ja, kan worden overgegaan tot het aangaan van een samenwerkingsrelatie. Die weging – of althans het resultaat daarvan – zal in de praktijk van dienst tot dienst kunnen variëren. Het is bovendien ook geen mathematische aangelegenheid. Naast de wettelijk vastgelegde criteria zullen ook concrete operationele belangen in relatie tot het door de diensten te beschermen belang van de nationale veiligheid een belangrijke rol kunnen spelen. Zoals de CTIVD heeft opgemerkt in rapport 22a dient de AIVD de grootst mogelijke terughoudendheid te betrachten in de samenwerking met diensten van landen waar nauwelijks tot geen democratische traditie bestaat en waar (structureel) mensenrechten worden geschonden, maar dat het op voorhand uitsluiten van samenwerking in de praktijk zou kunnen leiden tot onwenselijke of zelfs rampzalige situaties.[119] De Minister van BZK heeft in reactie hierop opgemerkt het standpunt van de CTIVD in beginsel te kunnen delen dat enkel in het geval van (concrete aanwijzingen voor) een terroristische dreiging met dergelijke diensten wordt samengewerkt, doch tevens gesteld dat er ook andere overwegingen spelen. De huidige diffuse dreigingssituatie vereist soms contacten met diensten die niet aan alle eisen voldoen. Dit geldt voor dreigingen richting Nederland maar in toenemende mate ook voor (mogelijke) dreigingen ten aanzien van Nederlandse belangen in het buitenland. In de weging wordt derhalve uiteindelijk bepaald waarom samenwerking met een partner – ook indien niet aan alle eisen wordt voldaan - noodzakelijk is, op welke wijze die samenwerking wordt ingevuld en welke randvoorwaarden daarbij gelden. In het kader van de weging zullen ook de risico's die aan een eventuele samenwerking verbonden zijn in kaart te worden gebracht. Dat bepaalt onder meer ook waaruit die samenwerking dan kan bestaan (en waaruit niet). Daarbij moet onder meer worden gedacht aan zaken als ten aanzien van welke onderwerpen onder welke omstandigheden gegevensuitwisseling kan plaatsvinden en aan welke andere voorwaarden moet worden voldaan. Het uitwisselen van persoonsgegevens verdient hierbij uitdrukkelijk de aandacht. Bij diensten waarvan is gebleken dat risico's

[119] CTIVD-rapport nr. 22a, blz. 9.

aan de samenwerking zijn verbonden wordt van oudsher terughoudendheid betracht bij het uitwisselen van persoonsgegevens. Uitgangspunt blijft dat op voorhand geen samenwerking kan worden uitgesloten. Met diensten die de mensenrechten onvoldoende respecteren vindt een uitdrukkelijke weging plaats aan de hand van de zwaarte van het belang dat met – een bepaalde vorm van – samenwerking is gemoeid. In artikel 76, vierde lid, van het wetsvoorstel is vastgelegd, dat de toestemming voor het aangaan van samenwerkingsrelaties met buitenlandse diensten in beginsel door de voor de dienst verantwoordelijke minister zelf dient te worden verleend; dus ongeacht of het gaat om risicodiensten of niet. Wel is er aanvullend in de mogelijkheid voorzien dat de minister de bevoegdheid tot het verlenen van toestemming aan het hoofd van de dienst mandateert. In dat geval geldt wel dat van een verleende toestemming de minister terstond op de hoogte dient te worden gesteld.

In artikel 76, vijfde lid, is ten slotte uitdrukking gegeven aan het feit dat samenwerking met buitenlandse diensten en de aard en intensiteit van die samenwerking in de loop der tijd aan verandering onderhevig kunnen zijn; zowel in positief als negatief opzicht. Zo kan, indien langer met een dienst wordt samengewerkt een steeds beter beeld van de betrouwbaarheid en professionaliteit worden gekregen. Dat kan ertoe leiden dat bij een dienst waarvan de betrouwbaarheid keer op keer is vastgesteld, de samenwerking een verdergaande vorm kan krijgen. Daartoe zal echter wel eerst opnieuw aan de hand van de genoemde criteria opnieuw een weging dienen te worden gemaakt. Het is met andere woorden een continu proces, waarbij een wijziging in de omstandigheden een nieuwe weging noodzakelijk maakt.

De AIVD en MIVD zullen, mede in het kader van het eerder genoemde artikel 75, elkaar ten behoeve van een zoveel mogelijk uniform Nederlands optreden op de hoogte houden van de afwegingen die zijn gemaakt in concrete gevallen.

Tot slot wordt nog het volgende opgemerkt. Artikel 76 geeft enkel een regeling ten behoeve van het aangaan van samenwerkingsrelaties en de aard en intensiteit daarvan. Dat laat onverlet dat bij iedere concrete handeling in het kader van die samenwerking, of die nu bestaat uit de verstrekking van gegevens of de inzet van bijzondere bevoegdheden in het kader van gezamenlijke operaties, telkens aan de daaraan gestelde eisen in de desbetreffende bepalingen zal moeten worden getoetst.

6.3.3 De verstrekking van gegevens alsmede het verlenen van technische en andere vormen van ondersteuning in samenwerkingsrelaties

In artikel 59, tweede tot en met zesde lid, van de Wiv 2002 is een regeling opgenomen, die het mogelijk maakt om – in andere gevallen dan waarbij de eigen goede

taakuitvoering van de dienst daartoe noopt[120] – aan een buitenlandse dienst gegevens te verstrekken dan wel daaraan technische of andere vormen van ondersteuning te verlenen. Deze regeling is in artikel 77 van het wetsvoorstel vrijwel gelijkluidend, maar wel met enkele belangrijke aanvullingen, opnieuw opgenomen. Daarnaast is ook een regeling opgenomen voor de omgekeerde situatie, namelijk ingeval door de AIVD of MIVD *aan* een buitenlandse dienst een verzoek tot technische of andere vormen van ondersteuning dient te worden gericht. Dit laatste is op dit moment ongeregeld, maar verdient mede in het licht van de discussie dat de AIVD en MIVD via tussenkomst van buitenlandse diensten bijzondere bevoegdheden zouden (kunnen) inzetten waartoe zij op grond van de Wiv 2002 niet gerechtigd zouden zijn, nadere normering.[121] Op beide regelingen zal thans nader worden ingegaan.

Artikel 77, eerste lid, bepaalt dat om het kader van een samenwerkingsrelatie als bedoeld in artikel 76 aan de desbetreffende dienst van een ander land gegevens kunnen worden verstrekt ten behoeve van door deze instanties te behartigen belangen, voor zover (a) deze belangen niet onverenigbaar zijn met de belangen die de diensten hebben te behartigen, en (b) een goede taakuitvoering door de diensten zich niet tegen verstrekking verzet. Opgemerkt wordt dat bij deze afweging de aard van de samenwerking met de desbetreffende buitenlandse collega-dienst, zoals die in het kader van artikel 76 is vastgesteld, medebepalend zal zijn. Op de verstrekking van gegevens zijn in artikel 77, derde lid, de artikelen 51, 55 en 56 van overeenkomstige toepassing verklaard. De verstrekking van gegevens in het kader van het eerste lid kan zowel betrekking hebben op gegevens die een of meerdere specifieke personen of organisaties betreffen, maar het kan ook gaan om ongeëvalueerde gegevens (veelal in grote hoeveelheden, de zgn. bulkdata). In de kabinetsreactie op het rapport van de commissie Dessens is aangegeven dat de uitwisseling van bulkdata met buitenlandse diensten zal worden onderworpen aan een systeem van ministeriële toestemming. Zoals ter toelichting op een vergelijkbare bepaling in artikel 49 van het wetsvoorstel is gesteld (zie par. 3.3.5.3.1), wordt afgezien van het gebruik "grote hoeveelheid" maar de toestemmingsregeling verbreed tot alle vormen van ongeëvalueerde gegevens. In artikel 77, tweede lid, wordt daarin voorzien. Wat hier onder ongeëvalueerde gegevens moet worden begrepen zijn bijvoorbeeld een kopie van een complete website en de in het kader van artikel 33 ontvangen en opgenomen gegevens waarop nog geen selectie is toegepast als bedoeld in artikel 35, eerste lid, van het wetsvoorstel. Overigens wordt opgemerkt dat de toestemming ook betrekking kan hebben op meerdere opeenvolgende verstrekkingen van vergelijkbare aard, zonder dat dit per geval dient te worden verleend.

[120] In dat geval vindt de gegevensverstrekking plaats op basis van artikel 36, eerste lid, onder d, Wiv 2002 (artikel 49, eerste lid, onder d, van het wetsvoorstel).
[121] Overigens heeft de CTIVD in rapport nr. 38 geconcludeerd dat hiervan geen sprake is.

Dat is met name van belang voor de uitwisseling van dergelijke gegevens in het kader van specifieke internationale samenwerkingsverbanden.

In artikel 77, vierde lid, is de mogelijkheid tot het verlenen van technische en andere vormen van ondersteuning geregeld. Daarbij is hetzelfde afwegingskader aan de orde als bij de verstrekking van gegevens. Voor het verlenen van de hier bedoelde ondersteuning dient een door de bevoegde autoriteit van de desbetreffende buitenlandse collega-dienst ondertekend schriftelijk verzoek aan de AIVD dan wel MIVD te worden gericht, waarin een nauwkeurige omschrijving wordt gegeven van de verlangde vorm van ondersteuning alsmede de reden waarom ondersteuning wenselijk wordt geacht. De verzochte ondersteuning wordt slechts verleend, indien – afhankelijk van de dienst waaraan het verzoek is gericht - daarvoor toestemming is verleend door de voor de desbetreffende dienst verantwoordelijke minister.

Evenals in het huidige artikel 59, zesde lid, is in artikel 77, zesde lid, voorzien in de mogelijkheid tot het verlenen van mandaat aan het hoofd van de dienst tot verlenen van toestemming naar aanleiding van het verzoek om technische en andere vormen van ondersteuning van een buitenlandse dienst. In de huidige wet is er enkel een mogelijkheid tot verlening van mandaat in spoedeisende gevallen. De CTIVD heeft in rapport 22a opgemerkt dat het enkele feit dat een bijzondere bevoegdheid wordt ingezet in het belang en ter ondersteuning van een buitenlandse dienst een verhoging van het toestemmingsvereiste naar het niveau van de minister niet *in alle gevallen* noodzaakt. Ook hierbij zou moeten gelden dat de toestemming om ondersteuning te verlenen aan een buitenlandse dienst die als risicodienst wordt aangemerkt door de minister wordt gegeven. In andere gevallen zou de bevoegdheid dan, ook in niet spoedeisende gevallen, bij het hoofd van de dienst kunnen komen te liggen. Voor de goede orde zij gesteld dat indien het verzoek om ondersteuning tevens betekent dat de inzet van bijzondere bevoegdheden plaatsvindt door de dienst, het regulier toestemmingsregime voor dit laatste blijft gelden.

In het wetsvoorstel wordt thans ook een regeling getroffen voor het doen van verzoeken om technische of andere vormen van ondersteuning door de AIVD of MIVD *aan* een buitenlandse collega-dienst. Het ontbreken van het toestemmingsvereiste voor het doen van een verzoek aan een buitenlandse dienst om ondersteuning was reeds eerder door de CTIVD in het eerder gememoreerde rapport nr. 22a (2009) gesignaleerd. De wet noch een interne regeling voorzag daarin. Ook de commissie Dessens wijst op het ontbreken van een regeling voor het doen van verzoeken aan buitenlandse diensten en verbindt daaraan de aanbeveling artikel 59 Wiv 2002 in dat licht te heroverwegen. Wij zijn het ermee eens dat niet valt in te zien waarom een verzoek *van* een buitenlandse dienst wel

expliciet is geregeld in de wet maar een verzoek *aan* een buitenlandse dienst niet. De desbetreffende regeling is in artikel 78 van het wetsvoorstel neergelegd.

Artikel 78, eerste lid, bepaalt dat de diensten in het kader van een goede taakuitvoering bevoegd zijn tot het doen van een verzoek om technische en andere vormen van ondersteuning aan inlichtingen- en veiligheidsdiensten van andere landen, indien daarvoor overeenkomstig het bepaalde in dit artikel toestemming is verleend. In artikel 78 wordt onderscheid gemaakt tussen een aantal situaties. Allereerst de situatie dat om ondersteuning wordt gevraagd bij de uitoefening van een bijzondere bevoegdheid, waarvoor reeds toestemming op grond van de wet is verleend: in dat geval wordt de toestemming verleend door degene de ingevolge het bij of krachtens artikel 24 bepaalde bevoegd is tot het verlenen van de toestemming voor de uitoefening van de desbetreffende bijzondere bevoegdheid (artikel 78, tweede lid). Concreet betekent dit, dat indien ingevolge de wet voor de uitoefening van een bijzondere bevoegdheid toestemming van de minister is vereist, de minister ook degene is die voor het verzoek om ondersteuning toestemming dient te verlenen. De uitoefening van de bijzondere bevoegdheid vindt in dit geval plaats binnen de Nederlandse jurisdictie en door de Nederlandse dienst zelf; zij kan daarbij echter in de uitvoering worden ondersteund door een buitenlandse dienst. Een andere situatie is, dat de ondersteuning die aan een buitenlandse dienst wordt gevraagd het verrichten van een handeling betreft die overeenkomt met de uitoefening van een bijzondere bevoegdheid als bedoeld in de paragrafen 3.2.2, 4.2 en 4.3 van het wetsvoorstel. Dan is hetgeen bij of krachtens deze paragrafen is bepaald van overeenkomstige toepassing. Concreet betekent dit, dat als de AIVD of MIVD aan een buitenlandse dienst een verzoek wil doen om bijvoorbeeld de telecommunicatie van een persoon in het desbetreffende land te intercepteren, daarvoor de regeling voor de toepassing van de bijzondere bevoegdheid tot het aftappen van telecommunicatie dient te worden toegepast. Dat betekent dat in dit voorbeeld er een gemotiveerd verzoek om toestemming aan de minister dient te worden voorgelegd. De verleende toestemming betekent tevens dat er toestemming is om aan de buitenlandse dienst het desbetreffende verzoek om ondersteuning te doen. Indien het in de twee geschetste situaties gaat om een geval waarbij het verzoek om ondersteuning niet in overeenstemming is met de aard en intensiteit van de samenwerkingsrelaties, zoals die naar aanleiding van de weging als bedoel in artikel 76 is vastgesteld, dient de toestemming altijd te worden verleend door de voor de dienst verantwoordelijke minister. Of door de desbetreffende buitenlandse collega-dienst de gevraagde ondersteuning wordt verleend, staat ter beoordeling van de voor die dienst verantwoordelijke autoriteiten die daarbij zelf zullen moeten beoordelen of het op hen van toepassing zijnde juridisch kader dat toestaat. Nederland is hierbij uitsluitend

verantwoordelijk voor het doe van het verzoek; indien de buitenlandse collega-dienst de verzochte ondersteuning verleent, moet deze geacht worden onder de verantwoordelijkheid van die dienst te worden uitgevoerd. In artikel 78, zesde lid, is bepaald dat van een verzoek om ondersteuning alsmede de verleende toestemming aantekening dient te worden gehouden. Dit is zowel van belang voor interne controle op de uitoefening van deze bevoegdheid als voor de uitoefening van de aan de CTIVD opgedragen taken.

In artikel 78, vijfde lid, is ten slotte bepaald dat een verzoek om ondersteuning als bedoeld in het derde lid geen betrekking kan hebben op het verrichten van handelingen die niet overeenkomen met de uitoefening van een bijzondere bevoegdheid als bedoeld in de paragrafen 3.2.2, 4.2 en 4.3 van het wetsvoorstel. Met deze regeling wordt aldus voorkomen dat men in de verzoeken om ondersteuning treedt buiten de bijzondere bevoegdheden die in de wet (limitatief) aan de diensten toekomen.

6.4 De samenwerking van de diensten met andere instanties

In paragraaf 5.2 van de huidige wet wordt een regeling gegeven voor de samenwerking van de diensten met andere instanties binnen Nederland. Deze regeling is grotendeels overgenomen in paragraaf 6.3 van het wetsvoorstel en op onderdelen aangevuld. De verschillende artikelen zullen thans nader worden toegelicht.

Artikel 79 van het wetsvoorstel treedt in de plaats van het huidige artikel 60 van de Wiv 2002. Dit artikel regelt de inschakeling van specifiek daartoe aangewezen ambtenaren bij de taakuitvoering van de AIVD. Deze inschakeling geschiedt onder verantwoordelijkheid van de Minister van BZK en overeenkomstig de aanwijzingen van het hoofd van de AIVD. De bestaande regeling wordt in het voorgestelde artikel 79 op twee onderdelen gewijzigd. De eerste wijziging betreft de uitbreiding van de kring van functionarissen waarop de regeling betrekking heeft. In artikel 60, eerste lid, van de huidige wet is thans bepaald dat de korpschef, de politiechef van een regionale eenheid, de commandant van de Koninklijke marechaussee en de directeur-generaal van de rijksbelastingdienst van het Ministerie van Financiën werkzaamheden verrichten ten behoeve van de Algemene Inlichtingen- en Veiligheidsdienst. De betrokkenheid van deze functionarissen bij de taakuitvoering van de AIVD en zijn voorgangers kent inmiddels een lange geschiedenis.

In het nieuwe artikel 79 wordt voorgesteld om ook de Hoofddirecteur van de Immigratie- en Naturalisatiedienst (IND) van het Ministerie van Veiligheid en Justitie alsmede de inspecteur-generaal van de Inspectie SZW van het Ministerie van Sociale Zaken en Werkgelegenheid onder de werking van artikel 79, eerste lid, te brengen. Dat betekent naast het feit dat deze functionarissen als zodanig ook taken voor de AIVD zullen

verrichten, dat de minister onder wie deze functionarissen ressorteren in overeenstemming met de Minister van Binnenlandse Zaken en Koninkrijksrelaties ondergeschikten van de Hoofddirecteur IND onderscheidenlijk de inspecteur-generaal van de Inspectie SZW zal dienen aan te wijzen die worden belast met de feitelijke uitvoering van en het toezicht op de werkzaamheden voor de AIVD. Deze werkzaamheden worden, zoals in artikel 79, derde lid, is bepaald, verricht onder verantwoordelijkheid van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en overeenkomstig de aanwijzingen van het hoofd van de AIVD. Aanwijzing van de Hoofddirecteur van de IND en daarmee ook de inschakeling van (aangewezen) medewerkers van de IND bij de taakuitvoering van de AIVD is aangewezen, omdat deze ambtenaren – eveneens als de reeds in het huidige artikel 60 opgenomen ambtenaren – een belangrijke "oog-en-oor"-functie voor de AIVD kunnen vervullen. Daar komt bij dat de IND sinds juli 2004 deelneemt in de zogeheten CT Infobox. De CT Infobox is een bijzonder samenwerkingsverband met als doel bij te dragen aan de bestrijding van terrorisme en radicalisme. Met de voorgestelde aanvulling wordt het mogelijk om de in de CT Infobox geplaatste medewerkers van de IND formeel als "artikel 60-functionarissen" aan te wijzen. Op dit moment worden de desbetreffende medewerkers door de AIVD overigens reeds als zodanig aangemerkt.[122] Sinds december 2010 neemt ook de Inspectie SZW deel aan de CT-Infobox. Op grond van artikel 79, tweede lid, kunnen derhalve ook de medewerkers van de Inspectie SZW die in de CT Infobox werkzaam zijn, worden aangewezen.

Een tweede wijziging is opgenomen in artikel 79, vierde lid. In het huidige artikel 60, vierde lid, is bepaald dat met betrekking tot het optreden van de ambtenaren van politie ter uitvoering van de in dit artikel bedoelde werkzaamheden hoofdstuk 7 van de Politiewet 2012 buiten beschouwing blijft. In dat hoofdstuk wordt een regeling gegeven voor de behandeling van klachten inzake het optreden van de politie. Indien de aangewezen politiefunctionarissen werkzaamheden verrichten voor de AIVD, dient daarop de klachtregeling zoals die in de Wiv 2002 is opgenomen van toepassing te zijn. Aangezien ook de ambtenaren van de KMar een politietaak hebben en daarop regulier de klachtregeling uit de Politiewet 2012 van toepassing is, dient deze eveneens in de situatie dat deze ambtenaren overeenkomstig artikel 79 werkzaamheden voor de AIVD verrichten buiten toepassing te worden verklaard.

Artikel 80 van het wetsvoorstel voorziet in een met artikel 79 van het wetsvoorstel vergelijkbare regeling waar het gaat om de inschakeling van de KMar ten behoeve van de taakuitvoering van de MIVD. Een dergelijke bepaling ontbreekt in de huidige wet. Zowel

[122] Verwijzing naar kabinetsreactie op rapport CTIVD inzake CT I.

de commissie Dessens[123] als de CTIVD[124] heeft de aanbeveling gedaan om de KMar ook werkzaamheden te kunnen laten verrichten op het militaire domein voor de MIVD. Er is voor gekozen om dit in een afzonderlijke bepaling te regelen en niet te incorporeren in het voorgestelde artikel 79. De relatie tussen de Minister van Defensie enerzijds en de KMar anderzijds bij het verrichten van bovengenoemde werkzaamheden ten behoeve van de MIVD is anders dan die tussen de Minister van BZK en de KMar bij het verrichten van werkzaamheden ten behoeve van de AIVD als bedoeld in artikel 79 (artikel 60 huidige wet). De Minister van Defensie is immers niet alleen verantwoordelijk voor het optreden van de MIVD, maar tevens degene die verantwoordelijk is voor het beheer van de KMar. Voorts verricht de KMar politietaken onder het gezag van de Minister van Veiligheid en Justitie (artikel 4, derde lid, van de Politiewet 2012), dan wel de burgemeester of de officier van justitie (artikel 14, eerste en tweede lid, van de Politiewet 2012). Deze taakuitvoering moet nadrukkelijk worden onderscheiden van het voorgestelde uitvoeren van taken ten behoeve van de MIVD. In artikel 80, eerste lid, wordt de commandant van de KMar van rechtswege aangewezen als een functionaris die werkzaamheden verricht ten behoeve van de MIVD; dit komt overeen met een vergelijkbare aanwijzing in artikel 79, eerste lid, maar dan voor de AIVD. In het tweede lid is aansluitend bepaald dat de Minister van Defensie ondergeschikten van de commandant KMar aanwijst tot de feitelijke uitvoering van en het toezicht op de aldaar bedoelde werkzaamheden. Deze werkzaamheden worden verricht overeenkomstig de aanwijzingen van het hoofd van de MIVD en onder verantwoordelijkheid van de Minister van Defensie (artikel 79, derde lid). Het betreft hier bijvoorbeeld werkzaamheden op luchthavens en grensovergangsplaatsen. In het vierde lid is ten slotte een met artikel 79, vierde lid, vergelijkbare regeling opgenomen, waarbij hoofdstuk 7 van de Politiewet 2012 buiten toepassing wordt verklaard met betrekking tot het optreden van de ambtenaren van de KMar ter uitvoering van de in artikel 80 bedoelde werkzaamheden.

De commissie Dessens en de CTIVD hebben met betrekking tot de werkzaamheden voor de MIVD aandacht gevraagd voor de afstemming met de AIVD waar het de inzet van de KMar betreft. Het spreekt voor zich dat de MIVD een leidende rol heeft bij aangelegenheden met een militaire relevantie. Dit vereist goede afstemming tussen beide diensten, temeer wanneer voor de feitelijke uitvoering van hun taken, beide diensten de KMar kunnen betrekken. Dit geldt vooral voor die onderwerpen ten aanzien waarvan zowel de AIVD als de MIVD activiteiten verrichten en waar derhalve van

[123] Rapport commissie Dessens, blz. 123.
[124] Brief van de CTIVD aan de Minister van Defensie van 27 september 2007 ten aanzien van de samenwerking tussen de MIVD en de KMar, waarin zij aanbeveelt om de KMar de bevoegdheid te geven om op een rechtstreekse manier werkzaamheden te verrichten op militair terrein ten behoeve van de MIVD.

dezelfde capaciteit gebruik moet worden gemaakt. Hiermee wordt onder meer ook bereikt dat de benodigde capaciteit op een efficiënte wijze wordt ingezet en verdeeld. Met betrekking tot de voorgestelde activiteiten is het voorgestelde artikel 75 van belang, ingevolge waarvan de diensten elkaar tijdig dienen te informeren over voorgenomen operationele activiteiten in Nederland en in andere landen, die naar verwachting van invloed kunnen zijn op een goede taakuitvoering van die andere dienst.

In artikel 81, eerste lid, is de verplichting voor de leden van het openbaar ministerie neergelegd om, door tussenkomst van het College van procureurs-generaal, dan wel, voor zover van toepassing, de procureur-generaal, bedoeld in de rijkswet openbare ministeries van Curaçao, van Sint Maarten en van Bonaire, Sint Eustatius en Saba, desgevraagd dan wel uit eigen beweging onverwijld mededeling te doen van gegevens die voor een dienst van belang kunnen zijn aan die dienst. Op dit moment is in artikel 61, eerste lid, reeds een informatieverplichting voor de hier bedoelde leden van het openbaar ministerie opgenomen. Deze is qua formulering in lijn gebracht met vergelijkbare aanpassingen in artikel 82, die deels al eerder waren voorzien in het ingetrokken post-Madridwetsvoorstel. Het is evident dat indien er sprake is van dergelijke gegevens, de mededeling daarvan – gelet op het in het geding zijnde belang van de nationale veiligheid – onverwijld dient plaats te vinden.[125] Teneinde elk misverstand daaromtrent te voorkomen, wordt voorgesteld dit nadrukkelijk in artikel 81, eerste lid, te stipuleren. In artikel 81, tweede lid, is, evenals in het huidige artikel 61, tweede lid, voorzien in overleg tussen het daar aangeduide lid van het openbaar ministerie en het hoofd van de desbetreffende dienst indien de taakvervulling van het openbaar ministerie dan wel de desbetreffende dienst daartoe aanleiding geeft.

Artikel 82 regelt een informatieverplichting voor de daarbij in het eerste lid aangewezen ambtenaren, welke thans is voorzien in artikel 62 van de wet. Ten opzichte van het huidige artikel 62 is artikel 82 in verschillende opzichten opnieuw geformuleerd. In artikel 82, eerste lid, wordt voor zover het gaat om de ambtenaren van de rijksbelastingdienst, de thans bestaande beperking “bevoegd inzake de douane” geschrapt. Daarmee komen dus alle ambtenaren van de rijksbelastingdienst onder de reikwijdte van de op grond van dat artikel geldende informatieverplichting te vallen. Deze wijziging wordt wenselijk geacht, opdat daarmee waardevolle informatie bij de rijksbelastingdienst die voor in het bijzonder het door de AIVD verrichte financieel onderzoek in de strijd tegen het terrorisme – anders dan op vrijwillige basis - beschikbaar kan komen. Om vergelijkbare redenen als uiteengezet bij de voorgestelde wijziging van artikel 81 is ook met betrekking tot de in artikel 82 neergelegde informatieverplichting bepaald, dat de

[125] Deze wijziging was reeds voorzien in het ingetrokken post-Madridwetsvoorstel.

mededeling (en verzending) van voor een dienst van belang zijnde gegevens onverwijld dient plaats te vinden. Een andere wijziging ziet op het expliciteren van de verplichting dat de gegevens ook *desgevraagd* verstrekt zouden moeten worden. Deze wijziging is opgenomen om onduidelijkheid betreffende de reikwijdte van de informatieplicht weg te nemen. Naar de huidige (letterlijke) formulering bezien wordt de informatieplicht (pas) geactiveerd op het moment dat de betreffende ambtenaar voor de dienst van belang zijnde informatie bij zijn taakuitvoering (spontaan) tegenkomt of althans daarvan kennis neemt. De vraag die in de toepassingspraktijk van het huidige artikel 62 zo nu en dan aan de orde komt is of de dienst gericht aan de betreffende ambtenaar om informatie kan vragen die deze dan vervolgens ook dient te verstrekken. Bij de parlementaire behandeling van de Wiv 2002 is door de regering ter zake opgemerkt: "Deze verplichting houdt ook in dat deze ambtenaren in voorkomend geval verplicht zijn mededeling te doen over gegevens in een door de politie gehouden register, indien een dienst hierom heeft verzocht in het kader van zijn taakuitvoering."[126] Deze uitspraak geeft een bevestigend antwoord op de hiervoor gestelde vraag. Daarnaast geldt dat indien de dienst aangeeft omtrent een bepaald onderwerp of bepaalde persoon informatie te willen ontvangen, dat daarmee de volgens het artikel (formeel) aan de ambtenaar toekomende afweging òf het voor de dienst van belang is niet meer aan de orde is; door de gearticuleerde vraag om informatie is dat belang immers gegeven. Met de voorgestelde wijziging wordt derhalve op wetsniveau duidelijkheid op dit punt geschapen. Aangezien deze problematiek zich ook bij de in artikel 81 geformuleerde informatieverplichting kan voordoen, is een vergelijkbare aanpassing daar aangebracht. Wel wordt hierbij opgemerkt dat de aldus ge(her)formuleerde informatieplicht zich in beginsel uitsluitend uitstrekt tot die gegevens waarover de betrokken ambtenaar in het kader van de uitoefening van zijn functie bevoegdelijk de beschikking kan krijgen (waarvoor hij is geautoriseerd). Tot slot is in artikel 82, tweede lid, voorzien in de mogelijkheid om – in afwijking van de in het (nieuwe) eerste lid voorziene wijze van verstrekken – de verstrekking van gegevens door de desbetreffende instantie tevens te laten plaatsvinden op rechtstreekse geautomatiseerde wijze. In het ingetrokken post-Madridwetsvoorstel was daar ook reeds in voorzien.[127] Het huidige artikel 62 van de Wiv 2002 voorziet daar thans niet in. Artikel 82, tweede lid, biedt aldus de mogelijkheid om, indien dat mogelijk en wenselijk is, op deze wijze aan de bestaande informatieverplichting te voldoen. In dergelijke gevallen zullen bij of krachtens algemene maatregel van bestuur nadere regels gesteld dienen te worden met betrekking tot de te treffen technische en organisatorische maatregelen; dat kunnen in dit geval zowel maatregelen zijn die dienen te worden

[126] Kamerstukken II 1997/98, 25 877, nr. 3, p. 75.
[127] Zie Kamerstukken I 2007/08, 30 553, A, artikel I onder U, artikel 62.

getroffen aan de kant van de desbetreffende dienst als maatregelen aan de kant van de instantie die de gegevens langs deze weg verstrekt.

In artikel 83 wordt een regeling getroffen voor het verlenen van technische en andere vormen van ondersteuning *door* de diensten *aan* de met opsporing en vervolging van strafbare feiten belaste instanties (eerste lid), *door* een of meer landelijke eenheden van de politie *aan* de diensten (tweede lid) alsmede *door* de KMar *aan* de diensten (derde lid). Op dit moment voorziet het huidige artikel 63 reeds in de mogelijkheid tot het verlenen van ondersteuning, echter deze is uitsluitend beperkt tot technische ondersteuning en ziet nog niet op de mogelijkheid dat door de KMar desgevraagd aan de diensten ondersteuning wordt verleend. In het ingetrokken post-Madridwetsvoorstel was een regeling opgenomen die (materieel) overeenkomt met hetgeen in artikel 83, eerste tot en met derde lid, wordt voorgesteld.[128] Met het verlenen van technische ondersteuning wordt bedoeld het ter beschikking stellen van technische apparatuur waarover de verzoekende instantie niet zelf beschikt dan wel voor zover deze er zelf over beschikt deze apparatuur reeds voor andere doeleinden wordt ingezet. Daartoe kan ook de ondersteuning door personeel worden gerekend, zij het dat die gerelateerd dient te zijn aan de verlangde technische ondersteuning. Gedacht moet worden aan bijvoorbeeld de beschikbaarstelling van personeel dat gespecialiseerd is in de bediening van de desbetreffende apparatuur. Waar het gaat om andere vormen van ondersteuning moet bijvoorbeeld worden gedacht aan het ter beschikking stellen van personeel dat bij volg- en observatie-activiteiten kunnen worden ingezet. In tegenstelling tot de huidige regeling, waarbij artikel 58, derde lid, van de Wiv 2002 van overeenkomstige toepassing is verklaard, is in de voorgestelde regeling de toe te passen procedure omtrent het doen van een verzoek bij de hier bedoelde bevoegdheden uitgeschreven. Daarmee wordt de bestaande onduidelijkheid ter zake weggenomen. Waar het gaat om een verzoek om ondersteuning door de diensten aan de met opsporing en vervolging van strafbare feiten belaste instanties, dient het schriftelijke verzoek daartoe door tussenkomst van het daartoe aangewezen lid van openbaar ministerie te worden ingediend. Daarmee wordt tevens bewerkstelligd dat de verzoeken de diensten via één kanaal bereiken en aldus voorkomen dat de dienst door telkens weer andere leden van het openbaar ministerie met verzoeken om ondersteuning wordt geconfronteerd. Indien door de dienst wordt bewilligd in het verlenen van de gevraagde ondersteuning, is het bevoegd gezag dat om de ondersteuning heeft verzocht vervolgens verantwoordelijk voor de feitelijke uitvoering van de te verrichten werkzaamheden (eerste lid, laatste volzin). Bij de verzoeken om ondersteuning als bedoeld in het tweede en derde lid, gaat het verzoek uit van de voor de dienst verantwoordelijke minister. Wel wordt thans in het vierde lid in de mogelijkheid

[128] Zie Kamerstukken I 2007/08, 30 553, A, Artikel I, onderdeel U, artikel 63.

voorzien dat in afwijking van het bepaalde in het tweede en derde lid in daarbij door de voor de desbetreffende dienst verantwoordelijke minister in door hem bepaalde gevallen en onder daarbij te stellen voorwaarden het verzoek om ondersteuning namens de minister door of namens het hoofd van de desbetreffende dienst wordt gedaan. Langs deze weg bestaat derhalve de mogelijkheid om – geclausuleerd – mandaat te verlenen, hetgeen in bepaalde gevallen van belang kan zijn om snel en flexibel te handelen. De desbetreffende minister wordt zo snel mogelijk omtrent aldus gedane verzoeken geïnformeerd. Waar het gaat om de verzoeken als bedoeld in het tweede en derde lid, geldt ook daar dat – ingeval de ondersteuning wordt verleend – de verantwoordelijkheid voor de feitelijke uitvoering bij de minister de om de ondersteuning heeft gevraagd komt te liggen.

6.5 Nadere regels inzake samenwerkingsverbanden

De diensten kunnen in het kader van een goede taakuitvoering samenwerkingsverbanden aangaan met een of meerdere instanties. Een voorbeeld daarvan betreft het samenwerkingsverband inzake de CT Infobox, waarbij op voet van gelijkwaardigheid door de daaraan participerende diensten en instanties wordt samengewerkt. Deze samenwerking vindt plaats onder het regime van de Wiv 2002 opdat op een optimale wijze gebruik gemaakt kan worden van bij de diensten beschikbare informatie. Het kan onder omstandigheden wenselijk zijn om ter zake van degelijke samenwerkingsverbanden nadere regels te stellen. Zo heeft de CTIVD in rapport nr. 12 (2007) inzake haar onderzoek naar de CT Infobox aanbevolen om de CT Infobox van een wettelijke basis te voorzien. Recent is de CT Infobox geëvalueerd. Nader zal moeten worden bezien of het inderdaad nog nodig is voor de CT Infobox een regeling te treffen.

Artikel 84, eerste lid, van het wetsvoorstel biedt – indien daaraan behoefte bestaat - de mogelijkheid daartoe. In het tweede lid wordt bepaald welke onderwerpen in een dergelijke nadere regeling in ieder geval opgenomen dienen te worden. Het betreft hier een omschrijving van het doel van het samenwerkingsverband, een aanduiding van de deelnemende organisaties, de taak en werkwijze van het samenwerkingsverband, de wijze waarop de afstemming tussen de diensten en deelnemende organisaties plaatsvindt alsmede de wijze waarop omtrent het functioneren van het samenwerkingsverband verantwoording wordt afgelegd.

Hoofdstuk 7 Toezicht, klachtbehandeling en de behandeling van meldingen van vermoedens van misstanden

7.1 Algemeen

Toezicht en controle op de activiteiten van de inlichtingen- en veiligheidsdiensten vindt zowel intern als extern plaats. Op de interne controle- en toezichtsmechanismen en de versterking daarvan mede in relatie tot het sturings- en coördinatievraagstuk, is reeds in hoofdstuk 2 van deze memorie van toelichting ingegaan. In dit hoofdstuk zal ingegaan worden op toezicht en controle door externe instanties. Daarbij zal allereerst in het kort geschetst worden hoe het huidige stelsel is ingericht (paragraaf 7.2). Dit stelsel blijft met uitzondering van het onderdeel toezicht en klachtbehandeling door de CTIVD en de rol van de Nationale ombudsman bij klachtbehandeling overigens ongewijzigd. Dat brengt met zich mee dat aansluitend slechts zal worden ingegaan op de voorstellen tot versterking van het toezichts- en klachtstelsel, zoals voorgesteld door de commissie Dessens, de reactie van de CTIVD daarop en de wijze waarop het kabinet heeft aangegeven daaraan uitwerking te willen geven.

7.2 Huidig stelsel extern toezicht

Extern toezicht en controle op de taakuitvoering van de diensten is in Nederland op dit moment belegd bij diverse instanties die ieder vanuit hun eigen optiek naar - verschillende aspecten van - die taakuitvoering kijken. Zo kunnen de volgende vormen worden onderscheiden: parlementaire controle, rechtmatigheidstoezicht door de CTIVD, klachtbehandeling door de Nationale ombudsman, controle op de financiële huishouding van de diensten door de Algemene Rekenkamer en toezicht door de rechter.

Parlementaire controle

De Ministers van BZK en van Defensie zijn volledig politiek verantwoordelijk voor de activiteiten van de AIVD onderscheidenlijk de MIVD en ter zake wordt sinds jaar en dag over de volle breedte verantwoording afgelegd tegenover het parlement. Parlementaire controle vindt zowel in het openbaar als besloten plaats. Openbare controle wordt uitgevoerd door met name de vaste commissies voor Binnenlandse Zaken (waar het gaat om AIVD-aangelegenheden) en voor Defensie (waar het gaat om MIVD-aangelegenheden) van de Tweede Kamer. Daarnaast is door de Tweede Kamer de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) ingesteld, die onder beding van geheimhouding parlementaire controle uitvoert op de geheime aspecten van de taakuitvoering van de diensten. Deze commissie bestaat uit de voorzitters van alle fracties die bij de laatste verkiezingen in de Tweede Kamer zijn verkozen.[129] De voorzitters van tussentijds ontstane fracties zijn niet in de CIVD vertegenwoordigd.

[129] Zie artikel 22, tweede lid, jo. artikel 11, eerste lid, Reglement van Orde voor de Tweede Kamer der Staten-Generaal.

De commissie Dessens heeft in haar rapport aangegeven dat – om de parlementaire controle effectief te doen functioneren - naar haar oordeel "openbaar, tenzij…" als uitgangspunt dient te gelden bij de informatieverstrekking aan het parlement. Dit uitgangspunt wordt door de regering gedeeld en is in het Algemeen Overleg dat met de Tweede Kamer is gevoerd over de evaluatie van de Wiv 2002 ook tot uitdrukking gebracht.[130] Met de commissie Dessens is de regering van oordeel dat bij het operationaliseren van het genoemde uitgangspunt sprake dient te zijn van een weloverwogen besluit aan de kant van de verantwoordelijke ministers welke informatie naar de betreffende vaste Kamercommissie kan gaan, waarmee het (in beginsel) openbaar wordt, en welke (geheime) informatie vertrouwelijk aan de CIVD wordt overgelegd. Het is inherent aan de taakuitvoering van inlichtingen- en veiligheidsdiensten dat omtrent bepaalde aangelegenheden, waarbij het actueel kennisniveau in het geding is dan wel sprake is van informatie die zicht geeft op dan wel betrekking heeft op bronnen en *modus operandi*, vanwege het staatsgeheime karakter daarvan slechts vertrouwelijk mededeling kan worden gedaan. In artikel 8, vierde lid, van de Wiv 2002, waarin de verplichting is neergelegd tot het uitbrengen van een verslag over de wijze waarop de AIVD en de MIVD hun taken in het afgelopen kalenderjaar hebben verricht, is dit ook wettelijk verankerd. Zo wordt informatie die zicht geeft op het actuele kennisniveau van de diensten en door de diensten aangewende middelen in concrete aangelegenheden sinds jaar en dag (uitsluitend) met de CIVD gedeeld.[131] Het bestaan van de CIVD heeft er mede toe geleid dat de verantwoordelijke ministers nooit informatie over de diensten aan het parlement hebben hoeven te weigeren met een beroep op het belang van de staat als bedoeld in artikel 68 Grondwet. Ook de commissie Dessens wijst hierop.

De informatie die vertrouwelijk aan de CIVD wordt verstrekt, mag door de leden van de CIVD niet met anderen worden gedeeld, ook niet met hun fractie. Dat gegeven geeft aan de te maken afweging door de ministers (openbaar of geheim) een extra gewicht, waarvan zij zich terdege bewust zijn. Aangezien de informatie die aan de CIVD wordt verstrekt omtrent een bepaald onderwerp veelal een gemengd karakter zal hebben, namelijk zowel vertrouwelijke als openbare informatie bevat, wordt bij het verstrekken van de informatie aan de CIVD aangegeven welke informatie vertrouwelijk en welke openbaar is. Op deze wijze is duidelijk welke informatie door de leden van de CIVD in voorkomende gevallen met bijvoorbeeld de fractiewoordvoerder op het terrein van inlichtingen- en veiligheidsdiensten kan worden gedeeld. Daar zit voor het kabinet

[130] Zie ook artikel 68 Grondwet: De ministers en de staatssecretarissen geven de kamers elk afzonderlijk en in verenigde vergadering mondeling of schriftelijk de door een of meer leden verlangde inlichtingen waarvan het verstrekken niet in strijd is met het belang van de staat.
[131] Zie artikel 8, vierde lid, Wiv 2002.

overigens wel een ondergrens aan, namelijk in die zin dat indien het onderwerp *als zodanig* in bepaalde gevallen geheim is, daar dan in het geheel niet buiten het verband van de CIVD over gecommuniceerd mag worden.

Vanuit de Tweede Kamer is aangegeven dat men wil onderzoeken of en, zo ja, op welke wijze de parlementaire controle op de inlichtingen- en veiligheidsdiensten eventueel anders ingericht zou kunnen worden. In het Algemeen Overleg over het evaluatierapport Wiv 2002 is door de Minister van BZK aangegeven dat het uiteraard aan de Tweede Kamer zelf is om te bepalen op welke wijze men de parlementaire controle wenst in te richten. Een voorstel ter zake van de zijde van de Tweede Kamer wordt dan ook afgewacht. Wel is door de Minister van BZK aangegeven dat het stelsel aan twee belangrijke criteria dient te voldoen. Allereerst dat daar waar geheimhouding dient te worden betracht, deze geheimhouding ook absoluut is gegarandeerd. Ten tweede dat het stelsel ook eenduidig is, en wel in die zin dat op voorhand helder is waar verantwoording wordt afgelegd over de activiteiten van de inlichtingen- en veiligheidsdiensten als zodanig en waar over andere aangelegenheden die als een afgeleide daarvan kunnen worden beschouwd, waarbij als voorbeeld is genoemd een reisadvies van de Minister van Buitenlandse Zaken dat is gebaseerd op een ambtsbericht van de AIVD.

Toezicht door de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD)

Met de inwerkingtreding van de Wiv 2002 werd in Nederland ook een nieuwe, onafhankelijke en gespecialiseerde toezichthouder op de activiteiten van de inlichtingen- en veiligheidsdiensten geïntroduceerd. In hoofdstuk 6 van de Wiv 2002, dat betrekking heeft op toezicht en klachtbehandeling, zijn onder meer de instelling, de samenstelling, de taakstelling, de bevoegdheden in het kader van het rechtmatigheidstoezicht en de verslaglegging omtrent de werkzaamheden van de CTIVD geregeld.

De CTIVD bestaat thans uit drie leden, en wordt bij de uitvoering van haar werkzaamheden ondersteund door een secretariaat. De leden van de CTIVD worden volgens een speciale in de wet nader uitgewerkte procedure benoemd. In die benoemingsprocedure speelt de Tweede Kamer een belangrijke rol, doordat de Kamer een lijst met kandidaten voor een vacature in de commissie voordraagt aan het kabinet, dat bij de keuze voor de persoon die de vacature gaat vervullen aan die voordracht is gebonden. Indien het kabinet geen van de voorgedragen kandidaten geschikt acht, vraagt het kabinet de Kamer om een nieuwe voordracht. Deze benoemingsprocedure in combinatie met het feit dat de toezichtsrapporten van de commissie (door tussenkomst van de verantwoordelijke minister) aan de beide kamers der Staten-Generaal worden aangeboden, markeert de bijzondere relatie tussen de CTIVD en het parlement. Met haar

toezichthoudende werkzaamheden draagt zij op een wezenlijke manier bij aan het effectueren van de parlementaire controle op de taakuitvoering van de diensten, zowel in het openbaar als in de beslotenheid van de CIVD.

De taken van de CTIVD zijn in artikel 64, tweede lid, van de Wiv 2002 omschreven. De hoofdtaak van de CTIVD vormt het toezicht op de rechtmatige uitvoering van hetgeen bij of krachtens de Wiv 2002 en de Wet veiligheidsonderzoeken (Wvo) is gesteld (artikel 64, tweede lid, aanhef en onder a, Wiv 2002). Voor de uitoefening van deze taak zijn aan de CTIVD vergaande bevoegdheden toegekend (paragraaf 6.2 Wiv 2002). Zo zijn de betrokken ministers, de hoofden van de diensten, de coördinator en voorts een ieder die betrokken is bij de uitvoering van de Wiv 2002 en de Wvo verplicht om desgevraagd alle inlichtingen te verstrekken en medewerking te verlenen die de CTIVD voor haar taak nodig heeft. De CTIVD heeft voorts recht op rechtstreekse toegang tot de gegevens die in het kader van de uitvoering van de Wiv 2002 en de Wvo worden verwerkt. De CTIVD kan onder meer ook getuigen en deskundigen om inlichtingen verzoeken en deze oproepen om voor haar te verschijnen en alle gevraagde inlichtingen te verstrekken. Voorts kan door de CTIVD worden bepaald dat een getuige niet eerder wordt gehoord dan nadat deze de eed of belofte heeft afgelegd.

De CTIVD bepaalt zelf waar zij onderzoek naar doet. In de wet is vastgelegd dat een dergelijk onderzoek ook kan worden verricht op verzoek van elk van beide kamers der Staten-Generaal. Dergelijke onderzoeken monden uit in openbare rapportages (met de mogelijkheid van een geheim deel) die door de desbetreffende ministers binnen 6 weken na de vaststelling door de CTIVD met een reactie aan beide kamers der Staten-Generaal worden verzonden; een eventueel geheim deel gaat met een reactie van de desbetreffende minister gelijktijdig naar de CIVD. Sinds haar bestaan (juli 2003) heeft de CTIVD reeds enkele tientallen toezichtsrapporten uitgebracht.[132]

Naast voornoemde taak heeft de CTIVD voorts tot taak:

- de verantwoordelijke ministers gevraagd en ongevraagd te informeren en adviseren over de door de commissie geconstateerde bevindingen. Desgewenst kan de CTIVD de betrokken minister vragen deze inlichtingen en adviezen ter kennis van een of beide kamers der Staten-Generaal te brengen, waarbij de werkwijze zoals beschreven in artikel 79 van overeenkomstige toepassing is;

- het adviseren van de betrokken minister ter zake van het onderzoeken en beoordelen van klachten;

[132] Voor een overzicht: zie de website van de CTIVD www.ctivd.nl

- het ongevraagd adviseren van de betrokken minister ter zake van de uitvoering van artikel 34 (notificatieplicht).

Van deze andere taken vormt het optreden als (verplichte) klachtadviesinstantie in het kader van de interne klachtbehandeling door de ministers in de praktijk de belangrijkste taak. Op de klachtbehandeling is de procedure in hoofdstuk 9 van de Algemene wet bestuursrecht van toepassing, zij het dat er op een enkel punt is voorzien in een afwijking (artikel 83, derde en vierde lid) waar het gaat om de klachtadvisering door de CTIVD.

De CTIVD dient ten slotte elk jaar voor 1 mei een openbaar jaarverslag uit te brengen van haar werkzaamheden.

Klachtbehandeling door de Nationale ombudsman

In artikel 83 van de Wiv 2002 is de klachtbehandeling expliciet in de handen van de Nationale ombudsman gelegd. In de praktijk ligt het zwaartepunt in de klachtbehandeling, maar dan als onderdeel van de interne klachtbehandeling, bij de CTIVD die, zoals hiervoor is geschetst, als (verplichte) klachtadviesinstantie optreedt. Klachten waaromtrent de CTIVD heeft geadviseerd en de minister heeft beslist, worden nog slechts bij uitzondering voorgelegd aan de Nationale ombudsman.

Controle door de Algemene Rekenkamer

De Algemene Rekenkamer is ingevolge de Comptabiliteitswet 2001 belast met rechtmatigheids- en doelmatigheidscontrole. In de artikelen 82 tot en met 96 van de Comptabiliteitswet 2001 worden daartoe regels gesteld. De Algemene Rekenkamer onderzoekt de doeltreffendheid en de doelmatigheid van het gevoerde beleid en de doelmatigheid van het financieel en het materieelbeheer, de daartoe bijgehouden administraties en de organisatie van het Rijk, en derhalve ook waar het gaat om de inlichtingen- en veiligheidsdiensten. Wat betreft de begrotingsartikelen *Geheim* van de diensten geeft artikel 87, derde tot en met vijfde lid, van die wet een specifieke regeling. Het onderzoek ligt dan in handen van de president van de Algemene Rekenkamer persoonlijk.

Controle door de rechter

Diverse aspecten van het werk van de inlichtingen- en veiligheidsdiensten kunnen onderworpen worden aan rechterlijke controle. Dat kan door de bestuursrechter, de civiele rechter of de strafrechter plaatsvinden. Zo kunnen bijvoorbeeld besluiten die de diensten nemen op basis van hoofdstuk 4 van de Wiv 2002 naar aanleiding van verzoeken om inzage in door of ten behoeve van de diensten verwerkte gegevens

alsmede de besluiten genomen op basis van de Wet veiligheidsonderzoeken (zoals de weigering of intrekking van een verklaring van geen bezwaar) worden voorgelegd aan de bestuursrechter. Het bestuursprocesrecht van de Algemene wet bestuursrecht is hierop van toepassing. Een natuurlijke persoon of rechtspersoon die woonplaats heeft onderscheidenlijk gevestigd is in de openbare lichamen Bonaire, Sint Eustatius of Saba, kan, indien hij belanghebbende is, beroep instellen bij het Gerecht in eerste aanleg van Bonaire, Sint Eustatius en Saba. De Wet administratieve rechtspraak BES is daarbij van overeenkomstige toepassing. De civiele rechter kan bijvoorbeeld worden geadieerd ingeval een burger van oordeel is dat door een dienst een onrechtmatige daad jegens hem is gepleegd.

Voorts kan de strafrechter in beeld komen indien een medewerker van de dienst zich als verdachte van het plegen van een strafbaar feit moet verantwoorden of als getuige in een strafproces moet optreden.

7.3 Versterking van het toezichts- en klachtstelsel

7.3.1 Het advies van de commissie Dessens

De commissie Dessens is in haar evaluatierapport uitvoerig ingegaan op het toezicht op de inlichtingen- en veiligheidsdiensten[133]; ook is zij ingegaan op de klachtbehandeling[134]. Zij plaatst een en ander met name in het licht van de eisen van het EVRM. De commissie is niet van oordeel dat het huidige stelsel niet voldoet maar acht het wel wenselijk daar wijzigingen in aan te brengen.

Waar het gaat om rechtmatigheidstoezicht stelt zij voor om de CTIVD als onafhankelijke toezichthouder de bevoegdheid te geven om een onmiddellijke toets op een verleende toestemming te laten verrichten en haar oordeel ter zake bindend te laten zijn. De commissie Dessens koppelt in haar rapport de versterking van het toezichtstelsel nadrukkelijk aan een uitbreiding van de bevoegdheid van de diensten tot ongerichte interceptie in het kabelgebonden domein. Overigens adviseert zij dit stelsel ook bij enkele andere bijzondere bevoegdheden toe te passen.[135] Een stelsel van preventief toezicht wordt door de commissie Dessens alles afwegende afgewezen. Waar het gaat om klachtbehandeling stelt de commissie voor om de CTIVD als een (zelfstandig)

[133] Zie de paragrafen 4.4 (extern toezicht) en 5.5 (extern toezicht op de inzet van bijzondere bevoegdheden) van het evaluatierapport.
[134] Zie paragraaf 7.4 (behandeling van klachten over de AIVD en de MIVD) van het evaluatierapport.
[135] Het betreft hier overigens allemaal bijzondere bevoegdheden waarvoor de minister zelf de toestemming moet verlenen, namelijk gerichte interceptie (artikel 25 Wiv 2002), selectie van ongericht ontvangen telecommunicatie (artikel 27, derde lid, Wiv 2002) en binnentreden in woningen (artikel 30).

onafhankelijke klachtinstantie te positioneren. Dus niet meer als klachtadviseur in de interne klachtbehandeling door de minister. De Nationale ombudsman blijft in het voorstel van de commissie bevoegd, maar zal zelf – zie artikel 9:23, onderdeel m, van de Algemene wet bestuursrecht - kunnen beslissen of voor hem nog een (rest)taak is weggelegd. De commissie Dessens merkt ten slotte op dat voor zover de beide (nieuwe) taken en bevoegdheden bij de CTIVD op gespannen voet met elkaar (kunnen) komen te staan, denkbaar is om bij de CTIVD een aparte klachtenkamer in te richten.

Het kabinet heeft het advies van de commissie[136] tot invoering van een bindend rechtmatigheidsoordeel door de CTIVD afgewezen. Bij de totstandbrenging van de Wiv 2002 is aangegeven dat de ministers volledig verantwoordelijk blijven voor de operationele activiteiten van de diensten en daarvoor ook ten volle verantwoording afleggen aan de beide Kamers der Staten-Generaal. Dit uitgangspunt brengt met zich dat aan de CTIVD niet de bevoegdheid is verleend om bindende besluiten te nemen ten aanzien van het opereren van de diensten. Mocht de CTIVD tijdens haar werkzaamheden op iets stuiten waarvan zij van mening is dat dit dient te stoppen dan kan zij de betreffende minister daarvan op de hoogte stellen. Het is vervolgens aan de minister om een besluit te nemen en daarover verantwoording af te leggen. Het toezichtsrapport van de CTIVD wordt immers openbaar gemaakt en voor zover er een geheime bijlage bij is gevoegd wordt die aan de CIVD toegezonden. Daar komt bij dat uit de toezichtspraktijk tot nu toe van de noodzaak tot invoering van een bindend rechtmatigheidsoordeel ook niet is gebleken. Waar het gaat om de klachtbehandeling neemt het kabinet het voorstel om de CTIVD als een (zelfstandige) onafhankelijke klachtbehandelaar te positioneren over.

De CTIVD heeft in haar reactie op het rapport van de commissie Dessens[137] positief gereageerd op het voorstel om aan de CTIVD de bevoegdheid tot het geven van een bindend rechtmatigheidsoordeel toe te kennen. Deze bevoegdheid zou – aldus de CTIVD – betrekking moeten hebben op alle bijzondere bevoegdheden, met uitzondering van die waarvoor een rechterlijke last is vereist[138]. De CTIVD ziet in de aanbeveling van de commissie Dessens een belangrijke waarborg ter versterking van haar rechtmatigheidstoezicht. Wel plaatst de CTIVD kanttekeningen bij het voorstel van een onmiddellijke toets. De CTIVD acht van belang dat sprake blijft van een vorm van toezicht achteraf door de CTIVD, waardoor haar positie in het proces niet ingrijpend

[136] Kamerstukken II 2013/2014, 33 820, nr. 2.
[137] Brief van de CTIVD aan de voorzitter van de Tweede Kamer d.d. 11 maart 2014.
[138] Vooralsnog is dat alleen bij het openen van brieven (uitvloeisel 13 Grondwet); in het wetsvoorstel tot wijziging van de Wiv 2002 inzake bronbescherming journalisten wordt tevens voorzien in vereiste van een rechterlijke last ingeval de diensten een bijzondere bevoegdheid jegens een journalist willen inzetten met het doel om – direct of indirect – diens bronnen te achterhalen.

wordt gewijzigd en de verantwoordelijkheid voor de keuze om een bijzondere bevoegdheid in te zetten duidelijk bij de diensten zelf en de verantwoordelijke ministers blijft liggen. De CTIVD wijst er verder op dat het onmiddellijkheidsaspect deels al onderdeel is van haar huidige werkwijze in het kader van rechtmatigheidstoezicht.[139] Het voorgaande neemt niet weg dat, aldus de CTIVD, uitbreiding van de staf van de CTIVD in dit kader aangewezen is.

In het Algemeen Overleg dat op 16 april 2014 met de vaste commissies voor Binnenlandse Zaken en voor Defensie over het kabinetsstandpunt is gevoerd, heeft de Minister van BZK, mede namens de Minister van Defensie, in aanvulling op het eerder uitgebrachte kabinetsstandpunt voorgesteld – om het stelsel EVRM-proof te doen zijn – de oordelen die de CTIVD gaat uitspreken in het kader van klachtbehandeling een bindend karakter te geven. Nu een bindend rechtmatigheidstoezicht, zoals door de commissie Dessens is voorgesteld, wordt afgewezen, wordt echter ter versterking van het toezicht op de toestemmingsverlening door de CTIVD een wettelijk vast te leggen heroverwegingsplicht voorgesteld. Dit houdt in dat als de CTIVD van oordeel is dat een door de minister verleende toestemming voor de inzet van een bijzondere bevoegdheid onrechtmatig is, de minister deze verplicht is opnieuw te bezien. Indien de minister van oordeel is dat de toestemming gehandhaafd moet blijven, dan dient de minister onverwijld de CTIVD en de CIVD daarvan op de hoogte te stellen. Op deze wijze kan de CIVD, indien zij daartoe aanleiding ziet, de minister ter verantwoording roepen. Aldus is sprake van een sluitend stelsel, waarbij de ministeriële verantwoordelijkheid intact wordt gelaten en tegelijk ook voorkomen wordt dat er praktijken ontstaan die onrechtmatig zijn zonder dat dit is getoetst. Tot slot is in het Algemeen Overleg van de zijde van het kabinet desgevraagd aangegeven dat waar het gaat om klokkenluiders van de diensten, de CTIVD daarin een rol kan spelen. Immers, bij de CTIVD kan men ook met staatsgeheime informatie terecht.

7.3.2 De uitwerking van het kabinetsstandpunt in het wetsvoorstel

In onderhavig wetsvoorstel is, langs de lijnen zoals die in het kabinetsstandpunt zijn aangegeven en met de Tweede Kamer zijn besproken, een voorstel opgenomen om de in de Wiv 2002 opgenomen regeling inzake toezicht en klachtbehandeling door de CTIVD te herzien. De belangrijkste wijzigingen betreffen: de inrichting en organisatie van de CTIVD, de uitbreiding van de reikwijdte van de algemene onderzoeksbevoegdheden in het kader van het toezicht tot de klachtbehandeling en de behandeling van meldingen inzake vermoedens van misstanden, de invoering van een heroverwegingsplicht voor de

[139] In het bijzonder bij het doorlopende onderzoek naar de inzet van de afluisterbevoegdheid en Sigint door de AIVD.

minister in het kader van het rechtmatigheidstoezicht, een integrale uitwerking van de nieuwe klachtprocedure met een bindend oordeel en – tot slot - een regeling voor de behandeling van meldingen van vermoede misstanden (klokkenluidersregeling).

De inrichting en organisatie van de CTIVD

In artikel 64, eerste lid, Wiv 2002 wordt de instelling van de CTIVD geregeld; in het tweede lid worden aansluitend de taken van de CTIVD gedefinieerd. In artikel 65, eerste lid, Wiv 2002 wordt bepaald dat de CTIVD uit een drietal leden bestaat; verder worden in dat artikel de aan de (te benoemen) leden te stellen eisen geformuleerd (twee van de drie leden dienen jurist te zijn) alsmede de wijze waarop de benoemingsprocedure is ingericht. In het huidige stelsel worden de in artikel 64, tweede lid, geformuleerde taken door de CTIVD als geheel uitgevoerd; dat betekent dat – voor zover hier relevant – rechtmatigheidstoezicht en klacht*advisering* is ondergebracht bij één, ongedeelde commissie. Dit is, nu de CTIVD in het kader van klachtbehandeling als adviseur optreedt en de uiteindelijke beslissing aan de minister is gelaten, ook niet problematisch.

In het nieuwe stelsel wordt de CTIVD als zelfstandige onafhankelijke klachtinstantie gepositioneerd, die bovendien tot voor de desbetreffende minister bindende klachtoordelen kan komen. Voorts zal de CTIVD worden belast met de behandeling van meldingen in verband met vermoede misstanden (klokkenluidersregeling). Dat roept de vraag op of vanuit de eis van onbevooroordeelde oordeelsvorming, zowel in het rechtmatigheidstoezicht als in de klachtbehandeling en de behandeling van vermoedens omtrent misstanden, de huidige situatie kan voortbestaan of dat er toch voorzien dient te worden in een organisatorische voorziening om de noodzakelijke onbevooroordeeldheid te borgen. Voorkomen moet worden dat commissieleden die in het kader van het rechtmatigheidstoezicht over een bepaalde kwestie hebben geoordeeld, over diezelfde kwestie tevens oordelen ingeval een klacht ter zake is ingediend dan wel ter zake het vermoeden van een misstand is gemeld. Ook de commissie Dessens heeft aan de kwestie aandacht besteed.[140] Ter zake merkt zij op dat in eerdere discussies als probleem naar voren is gebracht dat een toezichthouder die klachten over de diensten behandelt, strikt gesproken ook klachten over zichzelf afdoet. Voorts stelt zij dat dit argument wordt versterkt als het voorstel van de commissie wordt gevolgd, waarbij het rechtmatigheidsoordeel van de CTIVD in het kader van het toezicht een bindend karakter krijgt. Hoewel dit voorstel van de commissie Dessens niet wordt gevolgd, maar wel in een bindend klachtoordeel wordt voorzien, gaat deze vaststelling naar het oordeel van de regering hier evenzeer op. De in het wetsvoorstel opgenomen regeling neemt de door de commissie Dessens gesuggereerde oplossing van de instelling van een aparte

[140] Rapport van de Commissie evaluatie Wiv 2002, p. 151 e.v.

klachtenkamer (die door de commissie overigens niet verder wordt uitgewerkt) over en treft ter zake nadere voorzieningen met name qua samenstelling. Daarbij wordt tevens gehandeld in lijn met de jurisprudentie van het EHRM.

In de voorgestelde regeling worden bij de CTIVD twee afdelingen ingesteld: een afdeling toezicht en een afdeling klachtbehandeling (artikel 85, tweede lid).
De afdeling toezicht zal worden belast met: (a) het toezicht op de rechtmatigheid van de uitvoering van hetgeen bij of krachtens de Wiv 2002 en de Wet veiligheidsonderzoeken is gesteld, (b) het gevraagd en ongevraagd inlichten en adviseren van de betrokken Ministers aangaande de door de commissie geconstateerde bevindingen, waarbij de commissie desgewenst kan vragen deze inlichtingen en adviezen ter kennis van een of beide kamers der Staten-Generaal te brengen, waarbij de werkwijze zoals beschreven in artikel 101 van de wet van overeenkomstige toepassing is en (c) het ongevraagd adviseren van de betrokken ministers ter zake van de uitvoering van de notificatieplicht (artikel 85, derde lid).
De afdeling klachtbehandeling zal worden belast met (a) het onderzoeken en beoordelen van klachten en – dat betreft een nieuwe taak, waarop in het onderstaande nog separaat zal worden ingegaan - (b) het onderzoeken en beoordelen van meldingen van vermoedens van misstanden (artikel 85, vierde lid).
Anders dan de toezichtstaak is de taak met betrekking tot de klachtbehandeling (inclusief de behandeling van meldingen van vermoedens van misstanden) vraaggestuurd. Dit gegeven is mede bepalend geweest voor de verdere uitwerking van de twee afdelingen.
De afdeling toezicht bestaat uit drie leden, onder wie de voorzitter; daarbij wordt het voorzitterschap vervuld door de voorzitter van de CTIVD. De afdeling klachtbehandeling bestaat uit een voorzitter en ten minste twee andere leden. De voorzitter van de afdeling klachtbehandeling is tevens lid van de CTIVD; de andere leden van de afdeling klachtbehandeling zijn dat niet. De CTIVD komt aldus uit vier leden te bestaan (artikel 86, eerste lid). De voorzitter van de afdeling klachtbehandeling is niet tevens lid van – en neemt dus ook geen deel aan de uitoefening van het rechtmatigheidstoezicht door – de afdeling toezicht. Omgekeerd zijn de leden van de afdeling toezicht geen lid van de afdeling klachtbehandeling. Evenals bij de uitvoering van het rechtmatigheidstoezicht door de afdeling toezicht (en om vergelijkbare redenen), worden drie leden van de afdeling klachtbehandeling belast met de behandeling van klachten (en meldingen). Aan het aantal leden van de afdeling klachtbehandeling is in het wetsvoorstel geen limiet gesteld. Dit biedt de mogelijkheid om meerdere leden te benoemen (poolvorming) die aldus op een flexibele wijze kunnen worden ingezet. De leden van de afdeling klachtbehandeling zullen op een vergelijkbare wijze worden benoemd als de leden van de CTIVD, met dien verstande dat zowel de voorzitter als de overige leden van de afdeling

klachtbehandeling als jurist dienen te zijn gekwalificeerd (artikel 87, derde lid). Voor het overige zijn de bestaande bepalingen inzake incompatibiliteiten alsmede het op non-actief stellen en ontslag ook op de leden van de afdeling klachtbehandeling van toepassing. Bij algemene maatregel van bestuur zullen voorts nadere regels worden gesteld omtrent onder meer de bezoldiging en dergelijke (artikel 90).

De CTIVD alsmede haar afdelingen worden ondersteund door een secretariaat; artikel 91 geeft daarvoor een regeling. Om redenen die hiervoor zijn uiteengezet om tot de instelling van een afzonderlijke afdeling klachtbehandeling te komen, zal ook waar het gaat om de inrichting van het secretariaat daarbij aansluiting dienen te worden gezocht.

De uitbreiding van de reikwijdte van de algemene onderzoeksbevoegdheden in het kader van het toezicht tot de klachtbehandeling en de behandeling van meldingen inzake vermoedens van misstanden

In de huidige wet wordt waar het gaat om de bevoegdheden die de CTIVD toekomen bij de uitvoering van de aan haar opgedragen taken onderscheid gemaakt tussen bevoegdheden die van toepassing zijn in het kader van het rechtmatigheidstoezicht en het adviseren omtrent klachten. Zoals eerder in deze memorie van toelichting is aangegeven is op de behandeling van klachten, en ook op de advisering daaromtrent door een klachtadviesinstantie, de in hoofdstuk 9 van de Algemene wet bestuursrecht opgenomen regeling ter zake van toepassing. In artikel 83, derde lid, van de huidige wet is daartoe bepaald dat de betrokken minister alvorens zijn zienswijze te geven op een klacht, eerst het advies van de CTIVD dient in te winnen. Afdeling 9.1.3 Awb (Aanvullende bepalingen voor een klachtadviesprocedure) is daarbij van toepassing. Daarbij is tevens bepaald, dat de betrokken minister niet de bevoegdheid als bedoeld in artikel 9:14, tweede lid, Awb bezit, om aan de commissie algemene instructies te geven. Dat verdraagt zich immers niet met de onafhankelijke positie van de CTIVD, ook als klachtadviseur.

Overeenkomstig het kabinetsstandpunt naar aanleiding van het advies van de commissie Dessens, zal de CTIVD niet meer optreden als klacht*adviseur* maar worden gepositioneerd als een onafhankelijke, zelfstandige klachtinstantie. Bovendien krijgt de CTIVD in dat kader de bevoegdheid om jegens de minister bindende oordelen te geven. Deze nieuwe constellatie brengt met zich dat Afdeling 9.1.3 Awb niet meer van toepassing kan zijn; ook toepassing van titel 9.2 Awb kan niet aan de orde zijn, nu de CTIVD immers niet als ombudsman of ombudscommissie kan worden aangemerkt en voorts de CTIVD – anders dan een ombudsman – de bevoegdheid krijgt om bindende oordelen te geven. Een en ander betekent dat afzonderlijk voorzien moet worden in een

regeling van de (onderzoeks)bevoegdheden van de CTIVD in de sfeer van klachtbehandeling, in het bijzonder waar het gaat om toegang tot voor de klachtbehandeling noodzakelijke informatie alsmede een medewerkingsplicht. Geconcludeerd is dat de bestaande regeling ter zake in het kader van het rechtmatigheidstoezicht (paragraaf 6.2.1 Wiv 2002) zonder bezwaar ook onverkort van toepassing zijn bij de uitoefening van de nieuwe taak als onafhankelijke klachtinstantie. Een vergelijkbare conclusie is getrokken waar het gaat om de nieuwe taak van de CTIVD, te weten de behandeling van meldingen inzake vermoedens van misstanden. Paragraaf 7.2.1 van het wetsvoorstel voorziet in deze bevoegdheden. Gelet op het feit dat de CTIVD in een tweetal afdelingen wordt onderverdeeld, die ieder een eigen – van elkaar te onderscheiden – taak krijgen toebedeeld, worden de bevoegdheden in lijn daarmee aan de afdelingen (in plaats van aan de CTIVD als zodanig) toegekend.

De invoering van een heroverwegingsplicht voor de minister in het kader van het rechtmatigheidstoezicht

De CTIVD behoudt in het nieuwe stelsel haar taak om toezicht te houden op de rechtmatige uitvoering van de Wiv 2002 en de Wvo, zij het dat de uitvoering van die taak wordt belegd bij de afdeling toezicht van de CTIVD (artikel 85, derde lid, onder a). De bestaande wettelijke regeling voor de uitoefening van het rechtmatigheidstoezicht blijft ongewijzigd met dien verstande dat het onderzoek en daaraan gelieerde handelingen zijn opgedragen aan de afdeling toezicht. Het voorstel van de commissie Dessens om aan de CTIVD in het kader van het rechtmatigheidstoezicht de bevoegdheid toe te kennen om bindende oordelen te geven is, zoals eerder aangegeven, niet overgenomen. Wel is aangegeven dat anderszins zal worden voorzien in versterking van het toezicht op het verlenen van toestemming met betrekking tot de uitoefening van (bepaalde) bijzondere bevoegdheden, zonder dat daarbij de ministeriële verantwoordelijkheid wordt uitgehold. Daartoe wordt in het wetsvoorstel een wettelijke heroverwegingsplicht voor de minister geïntroduceerd (artikel 102 van het wetsvoorstel). Deze heroverwegingsplicht houdt het volgende in. Indien de afdeling toezicht in het kader de uitoefening van haar toezichthoudende taak tot de bevinding komt dat een door een minister verleende toestemming voor de uitoefening van een bevoegdheid als bedoeld in de artikelen 25, tweede lid (toepassing observatie- en registratiemiddelen in woningen), 27, derde lid (doorzoeken van woningen), 28, tweede en vierde lid (DNA-onderzoek; verdere verwerking resultaten DNA-onderzoek), 30, derde en zesde lid (verkennen van en binnendringen in geautomatiseerde werken; opleggen medewerkingsplicht bij ontsleuteling), 32, tweede lid (gericht afluisteren), 33, tweede lid (interceptie in bulk), 34, vierde lid (onderzoek aan in bulk geïntercepteerde gegevens), 35, tweede en vierde lid (selectie; metadata-analyse), 37, tweede lid (opleggen medewerkingspicht aan

aanbieder van communicatiedienst in het kader van toepassing artikel 33), 38, tweede lid (opleggen verplichting aan aanbieder van communicatiedienst tot verstrekken opgeslagen telecommunicatie) en 41, tweede lid (opleggen medewerkingsplicht bij ontsleuteling), niet in overeenstemming is met hetgeen bij of krachtens de wet is gesteld, kan zij de betrokken minister daarvan op de hoogte stellen. De minister is vervolgens verplicht zo spoedig mogelijk, doch uiterlijk binnen vijf werkdagen, naar aanleiding van een dergelijke mededeling het gewraakte besluit in het licht van de bevindingen van de afdeling toezicht opnieuw te bezien. Indien hij echter van oordeel is dat de bevindingen van de afdeling toezicht niet dan wel slechts ten dele tot heroverweging van zijn eerder verleende toestemming aanleiding geeft, moet hij daarvan terstond mededeling doen aan de afdeling toezicht alsmede aan de beide kamers der Staten-Generaal. Artikel 12, derde en vierde lid, van de wet, is daarbij van overeenkomstige toepassing verklaard. Dat betekent dat voor zover het gaat om vertrouwelijke gegevens deze mededeling aan de CIVD plaats dient te bevinden. Door de mededeling van de minister aan de beide kamers dan wel aan de CIVD, kan deze door het parlement – voor zover de mededeling in het openbaar is gedaan in het openbaar en voor zover vertrouwelijk aan de CIVD door de CIVD – ter verantwoording worden geroepen. De in het wetsvoorstel neergelegde heroverwegingsplicht strekt zich overigens niet uit tot alle bijzondere bevoegdheden, maar uitsluitend tot die bijzondere bevoegdheden waar de minister zelf toestemming voor dient te verlenen. Dat komt overeen met hetgeen de commissie Dessens in het kader van het door haar voorgestelde bindende rechtmatigheidstoezicht adviseerde. Uit het feit dat de toestemmingsverlening bij deze bevoegdheden in handen van de minister zelf is gelegd (met uitsluiting van mandaat), kan worden opgemaakt dat het daarbij gaat om bevoegdheden waarvan de uitoefening (potentieel) tot een grote inbreuk op de persoonlijke levenssfeer kunnen leiden. Het aan heroverweging onderwerpen van een bijzondere bevoegdheid waarvoor vanwege de veronderstelde geringe(re) inbreuk op de persoonlijke levenssfeer in mandaat, bijvoorbeeld door een teamhoofd of bewerker, de toestemming kan worden verleend, zou een met het beoogde doel disproportioneel middel zijn. Indien de heroverwegingsplicht wel het hele spectrum aan bijzondere bevoegdheden zou omvatten, zou niet alleen met betrekking tot die bevoegdheden waar thans geen toestemmingsvereiste geldt deze alsnog ingevoerd moeten worden, maar ook zou dan de opvolging naar aanleiding van een heroverweging opnieuw dienen te worden bezien.

Een integrale uitwerking van de nieuwe klachtprocedure met een bindend oordeel

In het wetsvoorstel wordt de CTIVD als een zelfstandige, onafhankelijke klachtinstantie gepositioneerd, waarbij het onderzoeken en beoordelen van klachten is opgedragen aan

de nieuw in te stellen afdeling klachtbehandeling bij de CTIVD. Ook het onderzoeken en beoordelen van vermoedens van misstanden (klokkenluidersrol) is, vanwege het met een klacht vergelijkbare karakter daarvan, bij die afdeling belegd. Op deze rol zal in navolgende paragraaf overigens nog afzonderlijk worden ingegaan. Zoals eerder in deze memorie van toelichting is aangegeven, kan de CTIVD niet worden beschouwd als een in titel 9.2 Awb bedoelde ombudsman of ombudscommissie, zodat de daarin geregelde procedure niet van toepassing is. Dat betekent dat daarvoor in een eigenstandige regeling dient te worden voorzien, waarbij overigens wel nauw aansluiting is gezocht bij de in de Awb geregelde procedure. Een belangrijk verschil met de in de Awb geregelde klachtprocedure is bovendien dat aan de afdeling klachtbehandeling van de CTIVD de bevoegdheid wordt toegekend om naar aanleiding van bij haar ingediende klachten tot voor de desbetreffende minister bindende oordelen te komen. Het toekennen van deze bevoegdheid betekent overigens niet dat de afdeling klachtbehandeling van de CTIVD ook wordt belast met het bindend beslissen van rechtsgeschillen tussen een burger en de overheid. Dat is en blijft de taak van de bestuursrechter en de burgerlijke rechter.

De klachtprocedure

Paragraaf 7.2.3 van het wetsvoorstel regelt de klachtprocedure. Hierbij is – ondanks het *sui generis* karakter van de klachtprocedure bij de CTIVD - zo nauw mogelijk aangesloten bij de regeling met betrekking tot de klachtbehandeling door een ombudsman (titel 9.2 Awb). Gelet hierop wordt afgezien van een inhoudelijke bespreking van de onderscheiden artikelen; voor de uitleg daarvan kan immers worden teruggevallen op die van de corresponderende artikelen in de Awb.

Zo is artikel 103 van het wetsvoorstel geënt op de artikelen 9:18 en 9:20 van de Awb, met dien verstande dat – in navolging van artikel 83 van de Wiv 2002 – zowel in artikel 103 als de overige bepalingen in paragraaf 7.2.3 wordt gesproken van ‘een klacht over het optreden of het vermeende optreden’ in plaats van ‘een verzoek om een onderzoek in te stellen naar een gedraging’. Evenals nu reeds in de huidige wet is voorzien, kan ook omtrent vermeend optreden worden geklaagd. Het is immers inherent aan onderzoeken door inlichtingen- en veiligheidsdiensten dat deze – om effectief te kunnen zijn – veelal op heimelijke wijze plaatsvinden, waarvan de klager vaak niet op de hoogte zal zijn. Ook zal niet altijd duidelijk zijn of een bepaald optreden aan bijvoorbeeld een van de diensten is toe te schrijven.[141] Het moet dan niettemin mogelijk zijn om een klacht in te dienen.

De artikelen 104, 105 en 106 hebben betrekking op de ontvankelijkheid van een klaagschrift, de onpartijdigheid van de klachtbehandelaar en op de mogelijkheid voor de

[141] Zie ook Kamerstukken II 1997/98, 25 877, nr. 3, blz. 94.

bij de klacht betrokken partijen om een toelichting te geven op de standpunten. Deze artikelen zijn ontleend aan de artikelen 9:28, 9:29 en 9:30 van de Awb.

Artikel 107 regelt, net als artikel 9:21 van de Awb dat doet voor de ombudsman, dat hoofdstuk 2 van de Awb in beginsel van toepassing is op het verkeer met de afdeling klachtbehandeling. Artikel 108 bevat, net als artikel 9:19 van de Awb, regels ter zake van een mogelijke samenloop met bezwaar, beroep of beklag.

De artikelen 109 tot en met 112 zijn ontleend aan de artikelen 9:22 tot en met 9:25 van de Awb en regelen onder welke omstandigheden de afdeling klachtbehandeling niet bevoegd onderscheidenlijk niet verplicht is een onderzoek in te stellen.

In het wetsvoorstel is – anders dan in titel 9.2 van de Awb (artikel 9:26) – niet voorzien in de mogelijkheid voor de afdeling klachtbehandeling om uit eigen beweging een onderzoek in te stellen. Daarvan is afgezien nu de klachtbehandeling kan leiden tot een bindend oordeel jegens de desbetreffende minister en dit spanning zou opleveren met de bevoegdheid van de CTIVD, in casu de afdeling toezicht, om uit eigen beweging een rechtmatigheidsonderzoek te starten, waarbij geen bindende oordelen kunnen worden uitgesproken.

Artikel 113 van het wetsvoorstel heeft betrekking op het oordeel van de afdeling klachtbehandeling. De afdeling klachtbehandeling beoordeelt of in de door haar onderzochte aangelegenheid rechtmatig en behoorlijk is gehandeld. Voorts kan de afdeling klachtbehandeling – anders dan een ombudsman op grond van titel 9.2 van de Awb – een bindend oordeel geven aan de betrokken minister. Aldus wordt een voorziening getroffen die – mede in combinatie met het toezicht door de afdeling toezicht van de CTIVD - een effectieve waarborg biedt tegen mogelijk misbruik van de aan de diensten toekomende bevoegdheden. De uitkomst van het onderzoek door de afdeling klachtbehandeling wordt zowel aan de klager als aan de betrokken minister medegedeeld. Bij de mededeling van haar oordeel aan de klager zal de afdeling klachtbehandeling deze, voor zover de veiligheid dan wel andere gewichtige belangen van de staat zich daartegen niet verzetten, met redenen dienen te omkleden (artikel 113, derde lid, van het wetsvoorstel). Dat legt op de afdeling klachtbehandeling een bijzondere verantwoordelijkheid, nu zij derhalve ervoor dient te waken dat door haar staatsgeheime informatie wordt geopenbaard. Bij het mededelen van haar oordeel aan de betrokken minister kan zij, ingeval zij tot het oordeel is gekomen dat in de door haar onderzochte aangelegenheid sprake is van een onrechtmatige of net behoorlijke gedraging, in verband daarmee tevens bepalen, dat indien en voor zover dat in verband staat met het desbetreffende optreden (a) een lopend onderzoek dient te worden gestaakt, (b) de uitoefening van een bijzondere bevoegdheid dient te worden beëindigd

of (c) door de diensten verwerkte gegevens worden verwijderd of vernietigd. Er is van afgezien om aan de afdeling ook de bevoegdheid tot het toekennen van schadevergoeding toe te kennen. Hiervoor zal de klager derhalve, met het oordeel van de afdeling klachtbehandeling in de hand, de civiele rechter kunnen adiëren. In artikel 113, vijfde lid, is vastgelegd dat de minister gehouden is het oordeel van de afdeling klachtbehandeling uit te voeren. Hij dient zowel de afdeling klachtbehandeling als de klager binnen twee weken na ontvangst van het oordeel schriftelijk op de hoogte te brengen van de wijze waarop hij aan dat oordeel uitvoering zal geven en binnen welke termijn.

Paragraaf 7.2.1 van het wetsvoorstel regelt in algemene zin de (onderzoeks)bevoegdheden van de afdeling klachtbehandeling, in het bijzonder waar het gaat om toegang tot voor de klachtbehandeling noodzakelijke informatie alsmede een medewerkingsplicht. Om die reden is in het wetsvoorstel geen pendant opgenomen van de artikelen 9:31 tot en met 9:36 van de Awb.

Gevolgen voor de Nationale ombudsman

Artikel 103 van het wetsvoorstel bepaalt dat titel 9.2 van de Awb niet van toepassing is. Dat betekent dat voor de Nationale ombudsman geen (rest)taak meer is weggelegd. Het wetsvoorstel wijkt in zoverre dus af van het advies van de commissie Dessens. Voor een (rest)taak voor de Nationale ombudsman ziet de regering geen aanleiding, nu de bevoegdheden van de afdeling klachtbehandeling, zowel met betrekking tot de te volgen procedure als met betrekking tot het oordeel, zoals hiervoor is toegelicht, aanzienlijk verder strekken dan die van de Nationale ombudsman.

7.4 De behandeling van meldingen inzake vermoedens van misstanden

In paragraaf 7.2.4 van het wetsvoorstel is de speciale procedure voor het melden van een vermoeden van een misstand voor (onder meer) ambtenaren werkzaam bij de AIVD en de MIVD uitgewerkt. Betrouwbaarheid en integriteit zijn onmisbaar voor een goed functionerende overheid en alle organisaties die daarvan deel uitmaken. Misstanden in ambtelijke organisaties doen daaraan afbreuk. Deze misstanden moeten worden voorkomen en als zij zich toch voordoen, worden beëindigd. Daarom moeten ambtenaren vermoedens van misstanden bij overheidsorganisaties kunnen melden zonder dat zij daarvan nadelen ondervinden. In artikel 125, quinquies, derde lid, van de Ambtenarenwet, wordt dit op de volgende manier tot uiting gebracht: "De ambtenaar die te goeder trouw de bij hem levende vermoedens van misstanden meldt volgens de procedure, bedoeld in het eerste lid onder f, zal als gevolg van het melden van die vermoedens geen nadelige gevolgen voor zijn rechtspositie ondervinden tijdens en na het

volgen van die procedure." Het ligt op de weg van de ambtelijke organisaties om meldingen van vermoedens serieus te nemen, te onderzoeken en, als zij juist blijken te zijn, de misstand te beëindigen. Voorwaarde voor het adequaat oplossen van misstanden is dat binnen de organisatie voor iedereen helder is hoe wordt omgegaan met vermoedens van een misstand.

In artikel 125quinquies van de Ambtenarenwet, wordt voor zover deze onderwerpen niet elders bij of krachtens de wet zijn geregeld de bevoegdheid verleend om regelingen te treffen voor onder meer de procedure voor een melding van een vermoeden van een misstand. Dit is reeds gebeurd in het Besluit melden vermoeden van misstand bij Rijk en politie (Stb. 2009, nr.572). In het kader van de bespreking van de evaluatie van de commissie Dessens echter "(….) heeft het kabinet net als de Tweede Kamer ongemak ervaren, zoals verwoord in het debat op 11 februari 2014. Het noodzakelijk heimelijke karakter van de diensten verhoudt zich slecht met het rechtzetten van misstanden in het openbaar."[142]

Daarom wordt nu in de momenteel aanhangige novelle op het voorstel van Wet Huis voor klokkenluiders (34105) voorgesteld om onder andere de coördinator en de ambtenaren die werkzaam zijn bij de Algemene Inlichtingen- en Veiligheidsdienst en de ambtenaren of militaire ambtenaren die zijn aangesteld bij de Militaire Inlichtingen- en Veiligheidsdienst uit te zonderen van het kunnen doen van een melding van een vermoeden van een misstand bij het Huis van de Klokkenluiders.

Om toch ook de ambtenaren bij de genoemde diensten in de gelegenheid te stellen een vermoeden van een misstand te kunnen melden, wordt in onderhavig voorstel in paragraaf 7.2.4 een voorziening getroffen speciaal voor hen. De ambtenaren bij de AIVD en de MIVD kunnen een melding doen bij de afdeling klachtbehandeling van de CTIVD.

De procedure sluit zoveel mogelijk aan bij de regeling voor andere ambtenaren, maar wijkt op onderdelen af gelet op de mogelijke gevoeligheid, vertrouwelijkheid of het geheime karakter van de werkzaamheden en de informatie van beide diensten. Hierna wordt ingegaan op de hoofdlijnen van de procedure zoals deze in onderhavig wetsvoorstel zijn opgenomen en op de elementen die afwijken van de reguliere procedure voor ambtenaren.

Het begrip "melder" wordt in artikel 114, onderdeel a, ruim gedefinieerd. Het is een ieder die betrokken is of is geweest bij de Wet op de inlichtingen en veiligheidsdiensten –of bij de Wet veiligheidsonderzoeken en die een melding doet. Voor deze ruime formulering is

[142] Kamerstukken II 2013/14, 33 820, nr. 3.

bewust gekozen. Daardoor kunnen niet alleen medewerkers van de diensten meldingen doen, maar bijvoorbeeld ook personen werkzaam bij telecombedrijven die betrokken zijn bij de uitvoering van taplasten en dergelijke. Op deze wijze wordt bewerkstelligd dat vermoedens van misstanden die gerelateerd zijn aan de uitvoering van beide wetten en waarbij mogelijk staatsgeheime informatie in het geding is bij een en dezelfde instantie terechtkomen, die daar dan ook effectief onderzoek naar kan doen. De afdeling klachtbehandeling heeft bijvoorbeeld toegang tot alle informatie bij de diensten. Aan de basis van een misstand ligt het feit dat een of meer betrokkenen zich niet hebben gedragen zoals het een goed ambtenaar betaamt, zoals omschreven in bijvoorbeeld artikel 125ter Ambtenarenwet en artikel 50 Algemeen Rijksambtenarenreglement. De in deze wet vervatte betrekkelijk zware procedure, waarbij een beroep kan worden gedaan op de onafhankelijke commissie van toezicht is bedoeld voor het aan de orde stellen van misstanden die van voldoende gewicht zijn en niet voor (vermoedens van) schendingen van lichte aard (artikel 117, eerste lid, onderdeel c, zegt dat een melding niet in behandeling wordt genomen als de afdeling klachtbehandeling van oordeel is dat het maatschappelijk belang bij een onderzoek door deze afdeling, dan wel de ernst van de misstand kennelijk onvoldoende is). Het begrip misstand wordt onderscheiden in een schending van wettelijke voorschriften, een gevaar voor de veiligheid of een gevaar voor het goed functioneren van de openbare dienst. Verdere definiëring is achterwege gelaten om geen onnodige drempels op te werpen voor potentiële melders

Het vermoeden van een misstand moet op redelijke gronden zijn gebaseerd. (artikel 114, onderdeel c). Uitgangspunt is bovendien dat de melder de melding eerst doet bij de organisatie waar de vermoede misstand zich afspeelt (artikel 115, eerste lid). Door deze interne procedure wordt de organisatie de mogelijkheid geboden de vermoede misstand adequaat te behandelen. Het vermoeden van een misstand dient dus eerst gemeld te worden bij een leidinggevende, een vertrouwenspersoon of een andere in een interne procedure aangewezen persoon. Indien de interne melding niet binnen een redelijke termijn of niet naar behoren is behandeld, kan een melder vervolgens bij de afdeling klachtbehandeling van de commissie van toezicht terecht. Een rechtstreekse melding bij de afdeling klachtbehandeling is ook mogelijk, als er omstandigheden zijn waardoor de melder niet terecht kan bij een van de genoemde personen binnen de dienst waarin de vermoedelijke misstand zich voordoet en van hem in redelijkheid niet gevraagd kan worden de interne procedure te doorlopen (artikel 115, tweede lid). In artikel 115, derde en vierde lid, is nader aangegeven wat de melding ten minste aan gegevens dient te bevatten en voorts dat de melder de voor de behandeling van de melding noodzakelijke gegevens dient te verstrekken waarover hij redelijkerwijs de beschikking kan krijgen.

De afdeling klachtbehandeling beoordeelt of de melding ontvankelijk is (artikel 116, eerste lid). De betrokken minister wordt in dat geval op de hoogte gesteld; de identiteit van de melder kan hem alleen na instemming van de melder worden meegedeeld (artikel 116, tweede lid). In artikel 117 is bepaald in welke gevallen de afdeling klachtbehandeling niet verplicht is om een onderzoek naar de melding in te stellen of voort te zetten. Indien de afdeling klachtbehandeling geen onderzoek instelt of dit niet voortzet, dient zij dit zo spoedig mogelijk gemotiveerd aan de melder en, voor zover de betrokken minister van de melding op de hoogte is gesteld, aan de minister te melden (artikel 118).

De afdeling klachtbehandeling onderzoekt of het aannemelijk is dat sprake is van een misstand en stelt naar aanleiding van het door haar verrichte onderzoek een rapport op (artikel 120). Ten behoeve van haar onderzoek staan de afdeling de bevoegdheden als bedoeld in paragraaf 7.2.1 van het wetsvoorstel ter beschikking. Voorts dient de afdeling klachtbehandeling, zowel de melder als de minister in de gelegenheid te stellen om hun standpunt toe te lichten (artikel 119).

In artikel 120, derde lid, is, in het kader van een zorgvuldige vaststelling van het rapport, bepaald, dat alvorens tot vaststelling van het rapport over te gaan de betrokken minister en de melder in de gelegenheid worden gesteld om op de bevindingen en het oordeel van de afdeling te reageren. Gelet op het feit dat de bevindingen van de afdeling mogelijk gevoelige gegevens bevatten, wordt de melder in de gelegenheid gesteld om deze bij de afdeling klachtbehandeling in te zien. Na de reactie van de minister en de melder wordt het rapport door de afdeling klachtbehandeling vastgesteld.

De afdeling klachtbehandeling deelt vervolgens de melder haar oordeel schriftelijk en, voor zover de veiligheid of ander gewichtige belangen van de staat er niet tegen verzetten, gemotiveerd mede. Ook de minister wordt daarvan op de hoogte gesteld; daarbij kan de afdeling naar aanleiding van het door verrichte onderzoek aan de minister aanbevelingen doen (artikel 120, zesde lid). Als de afdeling klachtbehandeling haar oordeel en eventuele aanbevelingen naar de betrokken minister zendt, dient deze binnen twee weken daarop de afdeling klachtbehandeling op de hoogte te stellen van de wijze waarop deze aan het oordeel gevolg zal geven en binnen welke termijn. De betrokken minister dient vervolgens zowel het oordeel als diens reactie daarop zo spoedig mogelijk aan een of beide Kamers der Staten-Generaal te zenden. Vanwege het geheime karakter zullen concrete feiten en omstandigheden niet bekend gemaakt worden, maar deze kunnen wel ter vertrouwelijke kennisneming aan een of beide Kamers der Staten-Generaal worden meegedeeld. In de praktijk betekent dit dat de CIVD van de Tweede

Kamer daarvan op de hoogte wordt gesteld. Op deze wijze kan de betrokken minister, indien de Kamer daartoe aanleiding ziet, ter verantwoording worden geroepen.

Hoofdstuk 8 Geheimhouding

Inlichtingen- en veiligheidsdiensten kunnen alleen effectief functioneren indien de werkzaamheden die door deze diensten in het kader van hun taakuitvoering worden verricht geheim zijn en – zolang dat noodzakelijk is – ook geheim blijven. Zowel in de huidige wet als in onderhavig wetsvoorstel zijn daarom diverse bepalingen opgenomen die geheimhouding van daarvoor in aanmerking komende informatie tot onderwerp hebben. Dat geldt in het bijzonder voor gegevens die betrekking hebben op het actuele kennisniveau van de dienst, de door de dienst aangewende middelen in concrete aangelegenheden alsmede de door de dienst aangewende geheime bronnen (zie onder meer artikel 12, derde lid, van het wetsvoorstel). Daarnaast rust op de hoofden van de dienst de plicht om zorg te dragen voor de geheimhouding van daarvoor in aanmerking komende gegevens alsmede van daarvoor in aanmerking komende bronnen waaruit gegevens afkomstig zijn (artikel 20 van het wetsvoorstel). Waar het gaat om menselijke bronnen is de geheimhouding bovendien ook absoluut. Zonder geheimhouding zou de bereidheid om als bron (informant/agent) voor een dienst te willen werken immers afnemen. In verband daarmee voorziet het wetsvoorstel dan ook nu in een regeling waarbij de identificerende gegevens van een menselijke bron op enig moment worden vernietigd. En ook in het kader van de regeling inzake de kennisneming van door of ten behoeve van de diensten verwerkte gegevens, zijn de nodige voorzieningen getroffen die ertoe strekken om gegevens die (vooralsnog) geheim dienen te blijven ook van kennisneming uit te sluiten. Daarnaast voorziet het wetsvoorstel, evenals de huidige wet, in een bijzondere geheimhoudingsregeling voor diegenen die bij de taakuitvoering van de diensten betrokken zijn (geweest) en uit dien hoofde kennis dragen over geheime informatie. Het betreft hier in het bijzonder de artikelen 124 en 125 van het wetsvoorstel (de huidige artikelen 85 en 86). Deze artikelen zijn in het wetsvoorstel in een aantal gevallen van overeenkomstige toepassing verklaard, teneinde de in deze artikelen neergelegde geheimhoudingsplichten ook tot de desbetreffende personente doen uitstrekken. Gewezen wordt onder meer op artikel 52, derde lid, en 54, derde lid, van het wetsvoorstel. Er is gekozen voor van overeenkomstige toepassingverklaring omdat de desbetreffende bepalingen zich niet direct tot de desbetreffende personen richten of dat daar onzekerheid over zou kunnen ontstaan. Immers artikel 124 richt zich tot een ieder die betrokken is bij de uitvoering van de wet en artikel 125 slechts tot ambtenaren die betrokken zijn bij de uitvoering van de wet. Met de van overeenkomstige toepassingverklaring wordt aldus de toepasselijkheid van de betreffende geheimhoudingsplichten op de desbetreffende personen en instanties buiten kijf gesteld.

Naast de hiervoor besproken geheimhoudingsbepalingen zijn in hoofdstuk 8 van het wetsvoorstel ook twee nieuwe bepalingen opgenomen, die deels het huidige artikel 87 van de Wiv 2002 vervangen. Artikel 126 ziet daarbij op bestuursrechtelijke procedures en artikel 127 op civielrechtelijke procedures. Ter toelichting wordt het volgende opgemerkt.

Artikel 126

Het huidige artikel 87, eerste lid, van de Wiv 2002 bepaalt dat in bestuursrechtelijke procedures inzake de toepassing van de Wiv 2002 of de Wet veiligheidsonderzoeken waarbij Onze betrokken Minister – lees: de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Defensie of de Minister-President, Minister van Algemene Zaken – of de commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten (CTIVD) door de rechtbank ingevolge de artikelen 8:27, 8:28 of 8:45 van de Algemene wet bestuursrecht (Awb) worden verplicht tot het verstrekken van inlichtingen dan wel het overleggen van stukken, artikel 8:29, derde tot en met vijfde lid, Awb buiten toepassing blijft. In artikel 8:29, derde tot en met vijfde lid, Awb is – kort gezegd – bepaald, dat de rechtbank beslist of de weigering van een partij om in verband met gewichtige redenen inlichtingen te geven dan wel stukken te overleggen dan wel de kennisneming van de inlichtingen of stukken uitsluitend te beperken tot de rechtbank, gerechtvaardigd is. Op grond van de huidige in artikel 87 opgenomen uitzondering beslist dus niet de rechtbank, maar de betrokken minister of de CTIVD over de geheimhouding van stukken.

In een uitspraak van 30 november 2011 (LJN BU6382) heeft de Afdeling bestuursrechtspraak van de Raad van State geoordeeld dat de rechter die een zaak beoordeelt, stukken die geheim zijn voor de betrokkene niet mag meewegen als de rechter niet heeft kunnen beoordelen of geheimhouding gerechtvaardigd is. Dat vloeit, aldus de Afdeling, voort uit de rechtspraak van het EHRM over het recht op een eerlijk proces zoals bedoeld in artikel 6 EVRM. Daarom heeft de Afdeling artikel 87, eerste lid, eerste volzin van de Wiv buiten toepassing gelaten voor zover volgens die bepaling de minister en niet de rechter beslist in hoeverre beperkte kennisneming van stukken gerechtvaardigd is. Door deze bepaling buiten toepassing te laten, komt de uitzondering die daarin wordt gemaakt op de regeling in artikel 8:29 van de Awb te vervallen. Dat betekent dat de rechter beslist of een beperkte kennisneming van stukken gerechtvaardigd is.

Voornoemde uitspraak heeft de commissie Dessens aanleiding gegeven in haar evaluatierapport de aanbeveling te doen om artikel 87 aan te passen aan de rechtspraak

over het recht op een eerlijk proces.[143] Het kabinet heeft deze aanbeveling overgenomen.[144]

In het nieuwe artikel 126 is de gewraakte uitzondering die in het huidige artikel 87 wordt gemaakt op de regeling in artikel 8:29 Awb geschrapt, waardoor artikel 8:29 Awb in volle omvang van toepassing wordt in bestuursrechtelijke procedures waar gegevens van de inlichtingendiensten een rol spelen. Zoals uit het voorgaande blijkt is de kern van deze bepaling dat de rechter beslist in hoeverre beperkte kennisneming van stukken gerechtvaardigd is. De Afdeling bestuursrechtspraak heeft in de meergenoemde uitspraak van 30 november 2011 geformuleerd hoe de rechter moet omgaan met deze discretionaire bevoegdheid. Volgens de Afdeling kan, indien de veiligheid van de staat in het geding is, het belang van die veiligheid een gerechtvaardigde grond zijn om de wederpartij kennisneming te onthouden van bewijsstukken waarvan de rechter wel kennisneemt. Zo'n beperkte kennisneming is, in het licht van de eisen die artikel 6 EVRM aan de eerlijkheid van het proces stelt, volgens de Afdeling evenwel slechts toelaatbaar als is voldaan aan de volgende voorwaarden. De rechter moet bevoegd zijn en in de gelegenheid worden gesteld te onderzoeken en te beslissen of zo'n beperkte kennisneming noodzakelijk en gerechtvaardigd is. Hij dient daarbij een afweging te maken tussen het belang van de staatsveiligheid dat wordt gediend met vertrouwelijkheid en het belang van de wederpartij bij kennisneming van het tegen haar ingebrachte bewijs. Bij die afweging betrekt de rechter de aard van de zaak en de resterende mogelijkheden voor de wederpartij om, overeenkomstig de eisen van een procedure op tegenspraak en gelijkheid van proceskansen, zijn standpunt in het geding te bepalen en naar voren te brengen. Aan de hand van die afweging dient de rechter te beoordelen of de onthouding van kennisneming gerechtvaardigd is. De beslissing die de rechter op basis van die beoordeling neemt, dient toereikend te zijn gemotiveerd.

Met het nieuwe artikel 126 wordt daarnaast bewerkstelligd dat ingeval de rechter een ander oordeel is toegedaan dan de betrokken minister of de CTIVD, de stukken door de rechter moeten worden teruggezonden aan de partij die ze heeft verstrekt dan wel overgelegd. De rechter moet die partij in de gelegenheid stellen zich te beraden of zij de inlichtingen alsnog wil verstrekken dan wel de stukken alsnog wil overleggen zonder het voorbehoud dat uitsluitend de rechter daarvan zal mogen kennisnemen. Indien die partij beslist dat zij de informatie niet zonder dit voorbehoud verstrekt dan wel de stukken niet zonder dit voorbehoud overlegt, kan de rechter daaruit ingevolge artikel 8:31 van de Awb de gevolgtrekkingen maken die hem geraden voorkomen. Dit betekent dat een oordeel van de rechter, dat het onthouden van geheime stukken aan een procespartij

[143] Zie het rapport van de commissie Dessens, paragraaf 7.5 (blz. 152 e.v.).
[144] Zie de kabinetsreactie op het rapport van de commissie Dessens van 11 maart 2014.

niet gerechtvaardigd is, niet leidt tot openbaarmaking van de geheime stukken door de rechter. Als de betrokken minister of de CTIVD ondanks het oordeel van de rechter volhardt in de geheimhouding van het stuk, kan dit wel leiden tot een verzwakking van hun procespositie. Met de nieuwe regeling in artikel 126, eerste lid, wordt uitdrukkelijk zeker gesteld dat de stukken ten aanzien waarvan een beroep op geheimhouding is gedaan door de betrokken minister of de CTIVD, weer retour naar de afzender komen. In het tweede lid van artikel 126 (nieuw) is door het van overeenkomstige toepassing verklaren van het eerste lid een soortgelijke regeling getroffen als hiervoor geschetst voor het geval de betrokken minister of de CTIVD door het Gerecht of het Hof ingevolge artikel 23, 28 en 29 van de Wet administratieve rechtspraak BES wordt verplicht tot het verstrekken van informatie.

De regeling in artikel 126, eerste en tweede lid, is naar zijn werking beperkt tot bestuursrechtelijke procedures inzake de toepassing van de Wiv en de Wet veiligheidsonderzoeken. Procedures waarbij derhalve de betrokken minister partij is. De problematiek waarvoor artikel 126 een oplossing geeft, is er echter niet alleen een die zich voordoet in de gevallen waartoe het huidige artikel 87 zich nu beperkt. Ook in de gevallen dat er geen sprake is van een bestuursrechtelijke procedure inzake de toepassing van de Wiv en de Wet veiligheidsonderzoeken kunnen de betrokken ministers op grond van artikel 8:45, eerste lid, Awb door de rechtbank worden verzocht tot het geven van schriftelijke inlichtingen of het inzenden van onder hen berustende stukken. Ingevolge artikel 8:45, tweede lid, Awb zijn bestuursorganen, ook als zij geen partij zijn, verplicht aan het verzoek te voldoen; artikel 8:29 Awb is daarbij van overeenkomstige toepassing verklaard. Daarbij moet worden gedacht aan bestuursrechtelijke procedures waarbij besluiten van andere bestuursorganen centraal staan, die (mede) gebaseerd zijn op door de diensten op de voet van artikel 36 Wiv 2002 verstrekte gegevens (ambtsberichten). Voorgesteld wordt dan ook om in het nieuwe artikel 126 een derde lid op te nemen, waarbij het eerste en tweede lid van overeenkomstige toepassing is ingeval een betrokken minister, niet zijnde partij in de bestuursrechtelijke procedure, wordt verplicht tot het geven van inlichtingen dan wel het overleggen van stukken in verband met door de dienst gedane mededelingen als bedoeld in artikel 49, eerste lid, onder a en b.

Artikel 126, vierde lid, (nieuw) tot slot komt overeen met het bepaalde in het huidige artikel 87, tweede lid, van de Wiv 2002. Indien door de betrokken minister of de CTIVD aan de rechtbank stukken dienen te worden overgelegd, kan worden volstaan met het ter inzage geven van de desbetreffende stukken. Daarmee wordt voorkomen dat die stukken – over het algemeen gaat het dan om rechtstreeks aan het dossier van een persoon ontleende documenten – buiten het bereik van de dienst dan wel de CTIVD geraken en

wellicht worden opgenomen in een procesdossier, hetgeen gelet op de zorgplicht die zowel de minister als de CTIVD heeft met betrekking tot de geheimhouding daarvan niet wenselijk is.

Artikel 127

De commissie Dessens heeft in haar evaluatierapport in overweging gegeven om de jurisprudentie over de omgang met geheime stukken in het civiele recht, net als voor het bestuursrecht, te codificeren.[145] Het nieuwe artikel 127 strekt daartoe. Op het terrein van het civiele recht regelt artikel 22 van het Wetboek van Burgerlijke Rechtsvordering de informatieplicht van partijen in civiele procedures. Uit deze bepaling volgt dat partijen het verstrekken van informatie kunnen weigeren als daarvoor gewichtige redenen zijn. Het artikel bepaalt niet meer dan dat de rechter beslist of sprake is van gewichtige redenen, 'bij gebreke waarvan hij daaruit de gevolgtrekking kan maken die hij geraden acht.' In artikel 22 wordt net als in artikel 8:29 Awb als materiële norm voor geheimhouding de aanwezigheid van 'gewichtige redenen' gehanteerd.

De Hoge Raad heeft in zijn arrest van 20 december 2002 (LJN AE 3350), bevestigd in een arrest van 11 juli 2008 (LJN BC 8421), aangegeven hoe ook in een civiele procedure naar analogie van de regeling in artikel 8:29 van de Awb met geheime informatie kan worden omgegaan. De benadering van de Hoge Raad is de volgende. Als een partij zich beroept op gewichtige redenen, dan dient de rechter in staat gesteld te worden te beoordelen of dat beroep terecht is. Dit betekent dat de desbetreffende partij de rechter vertrouwelijk in kennis zal moeten stellen van de desbetreffende inlichtingen of stukken. Als de rechter oordeelt dat er inderdaad sprake is van gewichtige redenen die een weigering tot het verstrekken van inlichtingen of het overleggen van stukken rechtvaardigen, dan vervalt de verplichting tot het geven van die inlichtingen of het overleggen van die stukken. Wel kan de desbetreffende partij de rechter meedelen dat alleen de rechter kennis zal mogen nemen van de door haar verlangde inlichtingen of stukken. De rechter zal in dat geval niet mede op grond van die inlichtingen of stukken uitspraak mogen doen dan nadat de wederpartij ondubbelzinnig daartoe toestemming heeft verleend. Wordt die toestemming niet verleend, dan kan de rechter die het geding verder behandelt, uit het niet verlenen van die toestemming de gevolgtrekking maken die hij geraden acht. In het geval de eerder bedoelde mededeling niet door eerstgenoemde partij wordt gedaan, of dat bedoelde toestemming niet door haar wederpartij wordt verleend, dan wel in het geval dat de rechter heeft geoordeeld dat geen gewichtige redenen aanwezig zijn voor de weigering doch de betrokken partij

[145] Zie het rapport van de commissie Dessens, paragraaf 7.5 (blz. 152 e.v.).

daarin volhardt, brengen volgens de Hoge Raad de eisen van een behoorlijke rechtspleging met zich mee dat de rechter die over de geheimhouding heeft beslist en in dat verband heeft kennisgenomen van de betrokken stukken of inlichtingen, niet deelneemt aan de verdere behandeling van het geding. De eventueel aan deze rechter ter beschikking gestelde stukken worden aan de partij die ze heeft verstrekt teruggeven. Deze procedurele garanties, die de Hoge Raad zoals hiervoor vermeld aan artikel 8:29 van de Awb heeft ontleend, zijn gecodificeerd in de leden een tot en met vier van het nieuwe artikel 127. Vanwege de beknoptheid van artikel 22 van het Wetboek van Burgerlijke Rechtsvordering is de civielrechtelijke procedure in artikel 127 wat meer uitgewerkt dan de bestuursrechtelijke procedure in artikel 126. De facto komen beide procedures voor de omgang met geheime informatie op hetzelfde neer: de vraag of geheimhouding van informatie gerechtvaardigd is, is ter beoordeling aan de rechter en als de rechter na kennisneming van de stukken van oordeel is dat geheimhouding niet gerechtvaardigd is, worden deze niet openbaar maar teruggezonden aan de partij die ze heeft verstrekt dan wel overgelegd.

Artikel 128

Artikel 128 is ongewijzigd gebleven ten opzichte van het huidige artikel 88. Kort gezegd wordt met deze bepaling bewerkstelligd dat in geval er een bezwaarschriftadviescommissie is ingesteld, deze commissie niet de bevoegdheid toekomt om ex artikel 7:13, vierde lid, Awb te beslissen over de toepasselijkheid van artikel 7:4, zesde lid, Awb. Dat betreft de vraag of ter inzage legging van de stukken achterwege dient te blijven omdat gewichtige redenen tot geheimhouding daartoe aanleiding geven. Indien de minister in een dergelijke procedure aan de commissie stukken overlegt en daarbij beroep doet op geheimhouding ervan, dient de beslissing over wel of niet ter inzage leggen aan de desbetreffende minister te worden voorbehouden. Deze bevoegdheid komt immers ook aan de minister toe ingeval het bezwaar zonder inschakeling van een adviescommissie wordt behandeld.

Hoofdstuk 9 Grondrechtelijke en mensenrechtelijke aspecten

9.1 Algemeen

De taken van de inlichtingen- en veiligheidsdiensten hebben vanwege hun aard betrekking op het privéleven van de personen waarnaar zij onderzoek doen. Het gaat immers om onderzoek naar onder meer de activiteiten van deze personen, de plannen die zij hebben, verblijfplaatsen en relaties. Ook de bevoegdheden die de diensten voor dit onderzoek ter beschikking staan, hebben in meer of mindere mate een impact op het privéleven van de betrokkenen. Denk aan observeren, het aftappen van telefoons, het

doorzoeken van besloten plaatsen en het doen van DNA onderzoek op basis van celmateriaal op voorwerpen. Het verzamelen en verwerken van gegevens, zowel persoonsgegevens als andere gegevens, vormt de kernactiviteit van de inlichtingen- en veiligheidsdiensten. Het verzamelen en verwerken van gegevens over het privéleven van burgers vormt een beperking van het recht op eerbiediging van de persoonlijke levenssfeer zoals neergelegd in artikel 10 van de Grondwet, artikel 8 van het EVRM en artikel 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke rechten (IVBPR). Het Handvest van de grondrechten van de Europese Unie is niet van toepassing op het handelen van de inlichtingen- en veiligheidsdiensten, aangezien het Handvest alleen van toepassing is op de terreinen die door het Unierecht worden bestreken en de nationale veiligheid gelet op artikel 4, tweede lid, van het Verdrag van de Europese Unie daarbuiten valt.

De persoonlijke levenssfeer (de term die wordt gebruikt in artikel 10 Grondwet) of het recht op het privéleven (dat in artikel 8 EVRM wordt gebruikt) is een ruim begrip waaronder diverse aspecten van het persoonlijke leven worden geschaard.[146] Een aantal in relatie tot de inlichtingen- en veiligheidsdiensten relevante aspecten van het recht op bescherming van de persoonlijke levenssfeer zijn in de Grondwet nader uitgewerkt in aparte rechten, zoals het recht op bescherming van het huisrecht (artikel 12 van de Grondwet) en het recht op bescherming van het brief-, telefoon- en telegraafgeheim (artikel 13 van de Grondwet). Deze rechten worden hieronder voor zover relevant afzonderlijk besproken.

Voor alle toepasselijke rechten geldt dat zij onder voorwaarden kunnen worden beperkt ten behoeve van de bescherming van de nationale veiligheid. De term nationale veiligheid is eveneens een ruim begrip. Er is geen definitie van gegeven, omdat dreigingen van de nationale veiligheid velerlei vormen kunnen aannemen en moeilijk op voorhand zijn te voorzien of af te bakenen. De reikwijdte ervan is echter uitgewerkt in jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM)[147]. Het begrip omvat in ieder geval de bescherming van de staatsveiligheid en de democratie tegen spionage, het schenden van staats- of militaire geheimen, steun voor of het verrichten van terroristische activiteiten, het oproepen tot geweld en de publicatie van geschriften die schade kunnen toebrengen aan het functioneren van de staatsveiligheidsdienst van een land. De bescherming van de nationale veiligheid omvat niet het opsporen van strafbare feiten.

[146] In het onderstaande zal overigens overwegend de term persoonlijke levenssfeer worden gehanteerd.
[147] Zie ook het Europees Hof voor de Rechten van de Mens, *'National security and European case-law'*, November 2013, beschikbaar op http://www.coe.int/t/dghl/standardsetting/dataprotection/judgments_EN.asp.

Elke beperking van het recht op bescherming van de persoonlijke levenssfeer ten behoeve van de nationale veiligheid dient te voldoen aan de vereisten die daaraan in de Grondwet, het EVRM en de jurisprudentie van het EHRM worden gesteld. In de Wiv 2002 en in het onderhavige wetsvoorstel is voorzien in een stelsel van waarborgen. In de wet is limitatief vastgelegd op welke wijze de diensten door gebruikmaking van de aan hen toegekende bevoegdheden een inbreuk mogen maken op het recht op bescherming van de persoonlijke levenssfeer van burgers. In alle gevallen moet daarbij worden voldaan aan de eisen van legitimiteit, noodzakelijkheid, proportionaliteit en subsidiariteit. Deze waarborgen zorgen ervoor dat de inbreuk op de persoonlijke levenssfeer die de inzet van bijzondere bevoegdheden in het belang van de nationale veiligheid tot gevolg kan hebben, in balans is met het recht op bescherming van de persoonlijke levenssfeer van de burger. Daarmee voldoet het wetsvoorstel aan de vereisten die de Grondwet en het EVRM stellen aan beperkingen van het recht op bescherming van de persoonlijke levenssfeer. Op deze waarborgen wordt hieronder in paragraaf 9.2 ingegaan.

Informatie van de AIVD en de MIVD kan in rechtszaken worden gebruikt. Vanwege het geheime karakter van de gegevens en de bevoegdheden die ter verkrijging of verwerking daarvan zijn ingezet, is het van belang om waarborgen op te nemen ten behoeve van de bescherming van het recht op een eerlijk proces. Het recht op een eerlijk proces is neergelegd in artikel 6 van het EVRM. Het houdt onder meer in dat als de Staat in een procedure voor de rechter een beroep op geheimhouding doet, de rechter moet onderzoeken of de onthouding van kennisname noodzakelijk en gerechtvaardigd is. De Afdeling bestuursrechtspraak van de Raad van State oordeelde in 2011 (LJN BU6382) dat de Wiv 2002 niet aan de eisen van artikel 6 EVRM voldoet, omdat in artikel 87, eerste lid, is bepaald dat niet de rechter, maar de Minister beoordeelt of bepaalde processtukken geheim moeten blijven. In artikel 126 van het wetsvoorstel wordt de regeling met betrekking tot geheimhouding van processtukken in bestuursrechtelijke procedures in lijn gebracht met de vereisten van artikel 6 EVRM. Een vergelijkbare voorziening wordt voor civielrechtelijke procedures getroffen in artikel 127. Deze regeling wordt besproken in hoofdstuk 8 van deze memorie van toelichting omtrent geheimhouding. Kortheidshalve wordt daarnaar verwezen.

Niet alleen het recht op een eerlijk proces dient te worden gewaarborgd, ook het recht op een daadwerkelijk rechtsmiddel (artikel 13 van het EVRM). Dat houdt in dat een onafhankelijke autoriteit met de bevoegdheid om bindende oordelen uit te spreken, klachten moet kunnen behandelen van burgers over de inlichtingen- en veiligheidsdiensten en passend herstel moet kunnen bieden. Hierop wordt ingegaan in paragraaf 9.3.

9.2 Het recht op eerbiediging van de persoonlijke levenssfeer

Zoals hierboven al aangegeven, omvat artikel 10 van de Grondwet het recht op bescherming van de persoonlijke levenssfeer. Bepaalde aspecten van het recht op bescherming van de persoonlijke levenssfeer zijn uitgewerkt in afzonderlijke artikelen in de Grondwet met een eigen beperkingsystematiek, maar artikel 10 van de Grondwet komt ook zelfstandige betekenis toe. Die aspecten van de persoonlijke levenssfeer die niet worden beschermd door de artikelen 11 tot en met 13 van de Grondwet, worden beschermd onder het algemene recht op bescherming van de persoonlijke levenssfeer van artikel 10 van de Grondwet. In de context van de nationale veiligheid moet dan worden gedacht aan de bevoegdheden van de diensten die zien op het observeren en volgen (artikel 25 van het wetsvoorstel; het inzetten van agenten en het doorzoeken van besloten plaatsen, niet zijnde woningen, voor zover daarbij een inbreuk wordt gemaakt op het privéleven (artikelen 26 en 27); DNA-onderzoek (artikel 28) en het verkennen van en binnendringen in geautomatiseerde werken voor zover daarbij een inbreuk wordt gemaakt op het privéleven (artikel 30). Deze bevoegdheden kunnen ook een inbreuk opleveren op het in artikel 8 EVRM neergelegde recht op bescherming van de persoonlijke levenssfeer. Conform de jurisprudentie van het EHRM raakt het verzamelen van informatie door autoriteiten over burgers zonder hun toestemming altijd hun privéleven en valt het daarmee binnen de bescherming van artikel 8 EVRM[148].

Hieronder wordt eerst het toetsingskader geschetst dat ingevolge artikel 10 van de Grondwet en artikel 8 EVRM van toepassing is op inbreuken op het recht op bescherming van de persoonlijke levenssfeer door de inlichtingen- en veiligheidsdiensten, en de wijze waarop de vereisten die uit dat toetsingskader volgen neerslag hebben gekregen in de Wiv 2002 en in het wetsvoorstel. Vervolgens wordt in de daaropvolgende paragrafen nog kort ingegaan op de specifieke eisen die gelden ten aanzien van de relevante aspecten van de persoonlijke levenssfeer die in de Grondwet aparte bescherming hebben gekregen (in artikel 10, tweede en derde lid; artikel 12 en artikel 13).

9.2.1 Toetsingskader

Artikel 10 van de Grondwet staat toe dat de wetgever bij of krachtens de wet beperkingen op het recht op eerbiediging van de persoonlijke levenssfeer stelt. Ook artikel 8 EVRM staat een inbreuk op het recht op bescherming van het privéleven toe als die inbreuk een legitiem doel dient, bij wet is voorzien en noodzakelijk is in een democratische samenleving. Artikel 17 van het IVBPR volgt voor wat betreft de

[148] *The right to respect for private and family life. A guide to the implementation of article 8 of the European Convention on Human Rights*, Ursula Kilkelly, Council of Europe Human Rights Handbooks no. 1, 2003.

voorwaarden waaronder het daarin neergelegde recht op eerbiediging van het privéleven mag worden beperkt dezelfde lijnen als artikel 8 van het EVRM. Artikel 17 van het IVBPR bevat geen expliciete eis dat beperkingen van het recht op bescherming van het privéleven bij wet moeten zijn voorzien, maar dit is zowel af te leiden uit de formulering dat 'niemand mag worden onderworpen aan willekeurige of onwettige inbreuken op zijn privéleven' als uit de *General Comments* van het VN Mensenrechtencomité, dat de naleving van dit verdrag controleert[149].

Basis in de wet

Een beperking van het recht op eerbiediging van de persoonlijke levenssfeer dient zoals gezegd een basis te hebben in de wet. Het EVRM vereist niet dat deze wettelijke basis is neergelegd in een formele wet. Ook gedelegeerde regelgeving, bekendgemaakte beleidsregels en vaste jurisprudentie kunnen volstaan.[150] De Grondwet vereist wel een formeelwettelijke basis voor inbreuken op de persoonlijke levenssfeer, al biedt artikel 10, tweede en derde lid, van de Grondwet de mogelijkheid om de uitwerking daarvan in lagere wet- of regelgeving te regelen. Het wetsvoorstel biedt dan ook, conform de grondwettelijke eis, een formeelwettelijke grondslag voor inbreuken op het privéleven. Daarmee wordt eveneens de democratische acceptatie van het wetsvoorstel gewaarborgd.

Het EHRM stelt twee nadere eisen met betrekking tot de kwaliteit van de wettelijke basis: de wet moet toegankelijk en voorzienbaar zijn (*accessible en foreseeable*)[151]. Toegankelijk wil zeggen dat de wetgeving gepubliceerd of bekend gemaakt is zodat burgers kunnen weten welke wetten er zijn. Voorzienbaar houdt in dat de wetgeving zodanig nauwkeurig is geformuleerd dat het mogelijk is voor burgers om de gevolgen te voorzien die de wetgeving voor hen heeft. Onder voorzienbaarheid volgt ook, ingevolge de jurisprudentie van het EHRM, dat de wetgeving voldoende waarborgen biedt tegen misbruik (ofwel verenigbaar is met de *rule of law*)[152].

De herziene wet wordt gepubliceerd en is daarmee voor iedereen toegankelijk. Daarmee wordt voldaan aan het vereiste van toegankelijkheid.

Voorzienbaarheid

[149] Human Rights Committee, General Comment nr 16.
[150] Intern beleid dat niet is gepubliceerd valt hierbuiten.
[151] EHRM 26 april 1979, *Sunday Times t. Verenigd Koninkrijk*, par. 49. Zie ook EHRM 24 april 1990, *Kruslin t. Frankrijk*, par. 30, EHRM 29 juni 2006, *Weber en Saravia t. Duitsland*, par. 84, EHRM 6 juni 2006, *Segerstedt-Wiberg en anderen t. Zweden*, par. 76.
[152] *Kruslin t. Frankrijk*, par. 33 en 35 en *Huvig t. Frankrijk*, 24 april 1990, par. 32 en 34.

Met betrekking tot de voorzienbaarheid van de wetgeving volgt uit de jurisprudentie van het EHRM[153] dat dit vereiste, gelet op de context waarin de inlichtingen- en veiligheidsdiensten opereren, niet zo ver gaat dat een persoon in staat moet zijn te voorzien wanneer een inlichtingen- of veiligheidsdienst zijn communicatie zou willen onderscheppen, zodat hij zijn gedrag daarop kan aanpassen. Om het risico van willekeur en misbruik tegen te gaan, moet de wet wel voldoende helder zijn in welke gevallen en onder welke voorwaarden de autoriteiten de bevoegdheid hebben om inbreuk te maken op het recht op eerbiediging van het privéleven en dient het toezicht daarop voldoende stevig te zijn. Dat betekent dat de wetgeving gedetailleerde regels moet geven voor het inzetten van bevoegdheden, zoals de interceptie van communicatie, waaronder regels die waarborgen bieden tegen misbruik en regels omtrent een onafhankelijke klachtenprocedure[154]. Deze nadere regels hoeven ingevolge de jurisprudentie van het EHRM niet in een wet in formele zin te zijn vastgelegd, maar mogen ook zijn uitgewerkt in lagere wetgeving of in openbaar gemaakte interne instructies[155].

In 2006 heeft het EHRM in het arrest Weber en Saravia t. Duitsland zijn jurisprudentie met betrekking tot het gericht aftappen van telecommunicatie (telefoontaps) verder uitgewerkt. In dit arrest geeft het EHRM de volgende minimum waarborgen die in wetgeving moeten zijn uitgewerkt om misbruik van (de interceptie)bevoegdheid te voorkomen[156]. In de wet moeten regels zijn opgenomen met betrekking tot: de aard van de gedragingen die tot de inzet van een interceptie bevoegdheid kunnen leiden; de categorieën van personen wier communicatie geïntercepteerd kan worden; een beperking van de duur van de interceptie bevoegdheid; de procedure die moet worden gevolgd voor het onderzoeken, gebruiken en opslaan van de gegevens die door middel van interceptie zijn verkregen; de voorzorgsmaatregelen die moeten worden getroffen als de gegevens met externen worden gedeeld en de omstandigheden waaronder gegevens moeten worden gewist of opnamen vernietigd.

Deze voorwaarden heeft het EHRM toegespitst op de gerichte interceptie van telecommunicatie, maar de voorwaarden zijn in brede zin van toepassing op andere bevoegdheden van de inlichtingen- en veiligheidsdiensten die een vergelijkbare inbreuk maken op het recht op bescherming van het privéleven, zoals in het geval van ongerichte interceptie en selectie[157]. Overigens heeft het EHRM in een latere zaak[158], waarbij het

---

[153] EHRM augustus 1984, *Malone t. Verenigd Koninkrijk*, par. 67, EHRM 26 maart 1987, *Leander t. Zweden*, par. 51.
[154] EHRM 4 mei 2000, *Rotaru t. Roemenië*, par. 59.
[155] EHRM 25 maart 1983, *Silver e.a. t. Verenigd Koninkrijk*, par. 88 en *Leander t. Zweden*, par. 51.
[156] *Weber en Saravia t. Duitsland*, par. 95, en het EHRM heeft deze criteria herhaald in EHRM 1 juli 2008, *Liberty e.a. t. Verenigd Koninkrijk*, par. 62, 63.
[157] EHRM 1 juli 2008, *Liberty en anderen t. Verenigd Koninkrijk*, par. 63.

ging om het via een GPS systeem volgen van de bewegingen van een persoon in de openbare ruimte, deze strikte standaarden niet toegepast. Volgens het EHRM is het volgen van bewegingen via een GPS systeem een minder vergaande inbreuk op de privacy van de betrokkene dan het afluisteren van diens telefoon waardoor met minder zware waarborgen zou kunnen worden volstaan. In het onderhavige wetsvoorstel worden waar mogelijk de zwaarste eisen als uitgangspunt gehanteerd, niet alleen voor gerichte interceptie maar voor alle bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten.

De hierboven genoemde eisen uit de arresten Weber en Saravia t. Duitsland en Uzun t. Duitsland dateren van na de inwerkingtreding van de Wiv 2002. In het wetsvoorstel is uitvoering gegeven aan zowel de vereisten die volgen uit Weber en Saravia t. Duitsland, als aan het - hierboven beschreven al eerder geformuleerde - vereiste dat de bevoegdheden in voldoende detail worden beschreven. Hieronder wordt dat nog nader toegelicht.

Waarborgen in het wetsvoorstel

Het EHRM vereist dat uit de wetgeving met voldoende duidelijkheid blijkt in welke gevallen de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten kunnen worden ingezet. In artikel 8 van het wetsvoorstel zijn de taken van de AIVD neergelegd; in artikel 10 van het wetsvoorstel de taken van de MIVD. Uit de opsomming die daarin is gegeven volgt dat beide diensten zich richten op dreigingen tegen de nationale veiligheid. Dit is dan ook leidend ten aanzien van het karakter van de gedragingen die tot de inzet van een bijzondere bevoegdheid kunnen leiden. Daarbij geldt dat de AIVD zich primair richt op organisaties en personen ten aanzien waarvan onderscheidenlijk ten aanzien van wie het ernstige vermoeden bestaat dat zij een gevaar vormen voor de nationale veiligheid, door de doelen die zij nastreven of door hun activiteiten. De diensten brengen jaarlijks aan het parlement een openbaar verslag uit van de aandachtsgebieden waarop zij zich in het afgelopen jaar hebben gericht en in het lopende jaar (in ieder geval) zullen richten. Niet alleen wordt op deze wijze op een voor een ieder kenbare manier aangegeven op welke wijze invulling is en wordt gegeven aan de aan de diensten toegekende wettelijke taak, maar kan deze tevens als basis dienen voor controle door het parlement of de diensten zich ook aan hun opdracht houden.[159]

---

[158] EHRM 2 september 2010, *Uzun t. Duitsland*, par. 66.

[159] Daarbij geldt wel de in artikel 12, derde lid, van het wetsvoorstel neergelegde beperking dat in het openbare jaarverslag in ieder geval de volgende gegevens achterwege blijven: door de diensten aangewende middelen in concrete aangelegenheden, door de dienst aangewende geheime bronnen en het actuele kennisniveau van de dienst. Deze informatie kan door de voor de dienst verantwoordelijke minister uitsluitend vertrouwelijk aan of beide kamers der Staten-Generaal

De bijzondere bevoegdheden van de diensten om gegevens te verzamelen en te verwerken mogen ingevolge artikel 23, eerste lid, echter niet voor alle taken van de inlichtingen- en veiligheidsdiensten worden ingezet, maar louter voor die taken waarbij het voor de effectiviteit ervan noodzakelijk is dat het onderzoek op een heimelijke wijze kan plaatsvinden. Het betreft hier de in artikel 8, tweede lid, onder a en d, en de in artikel 10, tweede lid, onder a, c en e, van het wetsvoorstel bedoelde taken. Voor deze beperking is gekozen vanwege de inbreuk die de bijzondere bevoegdheden kunnen maken op de persoonlijke levenssfeer van burgers[160]. Voor de overige taken van de inlichtingen- en veiligheidsdiensten (het verrichten van veiligheidsonderzoeken, de beveiliging bevorderende taak en het opstellen van dreigings- en risicoanalyses[161]) dienen zij zich te beperken tot de algemene bevoegdheid tot het verzamelen van gegevens die is neergelegd in artikel 22 van het wetsvoorstel; de in dit wetsvoorstel aan beide diensten opgedragen taak tot het doen van 'naslag' moet hiervan worden uitgezonderd, aangezien in dat kader geen gegevens (meer) worden verzameld, maar het gaat om een mededeling van door de diensten verwerkte gegevens omtrent een persoon of instantie. De beperking van de inzet van bijzondere bevoegdheden tot de uitvoering van een limitatief aantal taken van de diensten, was al geregeld in artikel 18 van de Wiv 2002. Hierin beoogt het wetsvoorstel geen verandering te brengen. Wel voorziet het wetsvoorstel in de mogelijkheid dat bijzondere bevoegdheden in een limitatief aantal gevallen ook mogen worden ingezet *ter ondersteuning* van de taakuitvoering van de diensten (artikel 23, tweede lid); een en ander strekt ter uitvoering van een aanbeveling van de commissie Dessens ter zake en is met strikte waarborgen omgeven (zie in het bijzonder artikel 24, vijfde lid).

In hoofdstuk 3 van het wetsvoorstel worden nauwkeurige regels gegeven voor de verwerking, waaronder begrepen de verzameling, van gegevens door de diensten, waardoor burgers kunnen weten in welke gevallen op welke wijze uitvoering kan worden gegeven aan een bevoegdheid en welke procedurele waarborgen daarbij gelden.

In paragraaf 3.1 worden enkele algemene bepalingen inzake de verwerking van gegevens (persoonsgegevens en andere gegevens) gegeven. In alle gevallen geldt daarbij de eis dat de verwerking van gegevens in overeenstemming met de eisen van de

---

worden medegedeeld (artikel 12, vierde lid); in de praktijk wordt deze informatie ter vertrouwelijke kennisneming aan de Commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer verstrekt.

[160] Kamerstukken 1997-1998, 25 877, nr.3, p. 26 en zie CTIVD, Toezichtsrapport nr. 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, 5 februari 2014, p. 55.

[161] Waar het gaat om de hier bedoelde analyses die door de AIVD en MIVD worden opgesteld, geldt dat in artikel 9, eerste lid, onderscheidenlijk 11, eerste lid, nader is bepaald welke gegevens daarbij mogen worden betrokken; artikel 9, tweede lid, onderscheidenlijk, 11, tweede lid, geeft een beperkte bevoegdheid aan de diensten tot het verzamelen van gegevens in dit kader.

Wiv of de Wvo dient plaats te vinden, dat deze plaatsvindt voor een bepaald doel en slechts voor zover noodzakelijk voor een goede uitvoering van de Wiv of de Wvo en in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze (artikel 17). In artikel 18 van het wetsvoorstel wordt onder meer de kring van personen weergegeven over wie gegevens mogen worden verwerkt. Ook geeft deze bepaling aanvullende eisen die worden gesteld aan de verwerking van bepaalde gevoelige gegevens, zoals iemands godsdienst of seksuele leven (derde lid), overeenkomstig de norm dat voor de verwerking van bijzonder gevoelige persoonsgegevens extra waarborgen dienen te zijn opgenomen (proportionaliteitseis). Ook worden diverse zorgplichten voor de hoofden van de inlichtingen- en veiligheidsdiensten gegeven, die er mede toe strekken dat de door de dienst verwerkte gegevens niet toegankelijk zijn voor niet daartoe geautoriseerde personen en voorts dat de volledigheid en de juistheid van de gegevens die worden verwerkt wordt geborgd. In paragraaf 3.2 wordt vervolgens een uitputtende regeling gegeven voor de verzameling van gegevens, waarbij onderscheid wordt gemaakt tussen de algemene bevoegdheid tot gegevensverzameling en de bijzondere bevoegdheden van de diensten. Naast de algemene eisen die zijn gesteld aan de uitoefening van bijzondere bevoegdheden (artikelen 23 en 24) worden voorts bij de afzonderlijke bijzondere bevoegdheden – waar dat gelet op de aard van de bevoegdheid is aangewezen – nadere, aanvullende waarborgen gesteld die beogen de uitoefening van de desbetreffende bijzondere bevoegdheid nader in te kaderen. Naast de vereisten van artikel 24, zesde lid, waar het gaat om de inhoud van een verzoek om toestemming, gaat het met name – waar dat gelet op de aard van de bevoegdheid mogelijk is – om een nadere invulling van de criteria zoals opgenomen in Weber en Saravia t. Duitsland. In het onderstaande zal daar nog nader op in worden gegaan.

In paragraaf 3.4 staan regels omtrent de interne en externe verstrekking van gegevens die met behulp van bijzondere bevoegdheden zijn verzameld en in paragraaf 3.5 over de verwijdering en vernietiging van deze gegevens.

Ten aanzien van bepaalde, bijzonder gevoelige gegevens zijn, zoals hierboven reeds aangegeven, extra waarborgen opgenomen met betrekking tot het bewaren en vernietigen ervan. Naast het bepaalde in artikel 18, derde lid, betreft het bijvoorbeeld ook het bewaren en vernietigen van celmateriaal en van de DNA-profielen die op basis daarvan zijn opgesteld. Op de bevoegdheid tot het verrichten van DNA onderzoek wordt hieronder nog nader ingegaan. Ten aanzien van de gegevens die worden verkregen door middel van het binnendringen in geautomatiseerde werken (hacken, artikel 30) of gerichte interceptie (artikel 32) zijn nieuwe bepalingen opgenomen die vereisen dat de deze gegevens zo spoedig mogelijk worden onderzocht op hun relevantie voor het onderzoek waarvoor ze zijn verworven. Niet-relevante gegevens en gegevens waarvan

de relevantie nog niet is vastgesteld, worden na een termijn van maximaal twaalf maanden vernietigd (artikel 30, negende lid en artikel 32, tiende lid). Dit is niet alleen een waarborg tegen misbruik van de bevoegdheid tot het verwerven van gegevens, maar ook van belang in de afweging of de inzet van een van deze bevoegdheden proportioneel is (zie hierna). Datzelfde geldt ten aanzien van de termijn van maximaal drie jaar waarin (ontsleutelde) gegevens die zijn verzameld door middel van de interceptiebevoegdheid ex artikel 33 van het wetsvoorstel mogen worden bewaard, waarna ze – indien ze niet relevant zijn dan wel niet op hun relevantie zijn onderzocht - moeten worden vernietigd. In paragraaf 3.2 van het wetsvoorstel worden de diverse bevoegdheden tot het verzamelen van gegevens geregeld; in paragraaf 3.2.1 de algemene bevoegdheid tot verzameling en in paragraaf 3.2.2 de bijzondere bevoegdheden. Het betreft een limitatieve opsomming. Per bijzondere bevoegdheid staat beschreven wat de omvang van de betreffende bevoegdheid is; ook is per bevoegdheid – vergelijk het bepaalde in artikel 24 in combinatie met de (aanvullende of afwijkende) regeling van de specifieke bijzondere bevoegdheid - voorzien in een regeling inzake de procedures die bij de uitoefening in acht moeten worden genomen ten aanzien van toestemming, duur van de toestemming, voor welke doeleinden de bijzondere bevoegdheid dient te worden uitgeoefend, wie toegang heeft tot de gegevens en de bewaar- c.q. vernietigingstermijn van de verworven gegevens. Daarbij geldt dat de waarborgen zwaarder worden naarmate het inbreukmakende karakter van een bijzondere bevoegdheid groter wordt[162].

Teneinde gevolg te geven aan het vereiste van het EHRM dat bevoegdheden voldoende kenbaar en voorzienbaar zijn, is, ook in navolging van adviezen van de CTIVD, een aantal bevoegdheden van een expliciete wettelijke basis voorzien. Het betreft bevoegdheden die al onder de bepalingen van de Wiv 2002 tot de bevoegdheden van de diensten werden begrepen, zoals het verrichten van DNA-onderzoek (artikel 28 van het wetsvoorstel) en de mogelijkheid om aan een verzoek om gegevens te voldoen door het verlenen van rechtstreekse geautomatiseerde toegang (artikel 22, derde lid, van het wetsvoorstel). In andere bepalingen is aangesloten bij de voortgeschreden technische en elektronische ontwikkelingen, zoals in artikel 33 van het wetsvoorstel, dat nu ook interceptie van kabelgebonden communicatie in bulk toestaat. Dit heeft eveneens tot gevolg dat de kenbaarheid en voorzienbaarheid van de wetgeving verder wordt vergroot.

Dat de waarborgen in het wetsvoorstel steeds zwaarder worden naarmate de inbreuk op de persoonlijke levenssfeer groter is, komt onder meer tot uiting in de toestemmingssystematiek. In artikel 24 van het wetsvoorstel worden algemene regels gegeven voor de toestemming. De uitoefening van een bijzondere bevoegdheid als

[162] CTIVD rapport nr. 38, p. 54.

bedoeld in paragraaf 3.2.2 van het wetsvoorstel is slechts toegestaan indien, voor zover niet anders bepaald, de betrokken minister of namens deze het betrokken hoofd van de dienst daartoe toestemming heeft gegeven. Dit maakt het mogelijk voor de betrokken minister om volledige ministeriële verantwoordelijkheid te dragen voor de inzet van bijzondere bevoegdheden door de betreffende inlichtingen- en veiligheidsdienst en daarover parlementaire verantwoording af te leggen. Het verzoek om toestemming en een eventueel verzoek om verlenging daarvan omvatten onder meer het beoogde doel van de uitoefening van de bevoegdheid en de reden waarom de uitoefening noodzakelijk wordt geacht. Voor de bevoegdheden die een grotere inbreuk maken op het privéleven is voorzien in een afwijkende toestemmingsregeling, afhankelijk van de mate en ernst van de inbreuk die de bijzondere bevoegdheid kan maken op de persoonlijke levenssfeer. Voor de meest inbreukmakende bevoegdheden is toestemming van de minister nodig, zonder mogelijkheid van mandatering aan het hoofd van een dienst of aan een door het hoofd aangewezen ambtenaar. Het gaat om de toepassing van observatie- en registratiemiddelen binnen de woning (artikel 25 van het wetsvoorstel); het doorzoeken van woningen (artikel 27); het doen van DNA-onderzoek en het verlengen van de bewaartermijn van een DNA-profiel (artikel 28); het verkennen van en binnendringen in geautomatiseerde werken (artikel 30); onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers (artikel 32); onderzoek van communicatie in andere gevallen zoals bedoeld in artikelen 33 en 34 van het wetsvoorstel; de selectie van gegevens die zijn verzameld met behulp van de bevoegdheid ex artikel 33 alsmede metadata-analyse gericht op het identificeren van personen en organisaties (artikel 35); het verzoeken om medewerking aan aanbieders van communicatiediensten voor zover die medewerking inbreuk maakt op het privéleven van de betrokkene (artikelen 37 en 38); en het verzoeken om medewerking aan het ontsleutelen van gegevens (artikel 41).

Voor het openen van brieven en andere geadresseerde verzendingen is ingevolge artikel 13 van de Grondwet voorafgaande toestemming van – in casu – de rechtbank Den Haag vereist (artikel 29, eerste lid). Dit is ook het geval indien de bijzondere bevoegdheden worden ingezet jegens journalisten met het doel hun bronnen te achterhalen (artikel 24, vierde lid). Dit laatste vereiste vloeit voort uit de uitspraak van het EHRM in de zaak Telegraaf Media Groep t. Nederland, waarin het EHRM heeft geoordeeld dat artikelen 8 EVRM en 10 EVRM (recht op vrije meningsuiting) werden geschonden doordat de nationale wetgeving niet voorziet in voorafgaande toetsing van de inzet van bijzondere bevoegdheden door de inlichtingen- en veiligheidsdiensten, gericht op het achterhalen van de bronnen van journalisten[163]. In hoofdstuk 3 van deze memorie van toelichting is

[163] EHRM 22 november 2012, *Telegraaf Media Groep t. Nederland*.

nader ingegaan op deze uitspraak en de wijze waarop de regering daaraan uitvoering geeft.

In artikel 24 van het wetsvoorstel is opgenomen dat de toestemming, tenzij anders bepaald, voor een periode van hoogstens drie maanden wordt gegeven en alleen op verzoek telkens voor eenzelfde periode kan worden verlengd. Dit is conform het hierboven genoemde vereiste in de jurisprudentie van het EHRM dat er in de wettelijke regels een limiet moet zijn gesteld aan de inzet van bevoegdheden. Het EHRM stelt geen eisen aan de duur van deze limitering, anders dan dat deze in elk geval proportioneel dient te zijn. De regering kiest ervoor de uitoefening van een bijzondere bevoegdheid in principe tot de korte periode van drie maanden te beperken. Waar een langere periode van toestemming is voorzien, is deze periode ingegeven door praktische overwegingen, zoals de complexiteit van het onderzoek[164], in samenhang met de mate waarin deze bevoegdheid inbreuk maakt op de persoonlijke levenssfeer van burgers, zoals bijvoorbeeld bij de interceptie ex artikel 33 van het wetsvoorstel. De limitering van de duur van de inzet draagt ook bij aan de proportionaliteit van de inzet van bevoegdheden: hoe indringender inbreuk wordt gemaakt op de persoonlijke levenssfeer, hoe korter de duur van de toestemming. De proportionaliteit van de inzet wordt ook getoetst bij het verzoek om toestemming, door de doelbeschrijving en de motivering van de inzet dan wel de verlenging (zie daarover ook hieronder).

Een andere waarborg tegen misbruik is de weerslag van het 'need to know'-principe dat is neergelegd in artikel 48 van het wetsvoorstel inzake de interne verstrekking van gegevens. Dit houdt in dat interne verstrekking van gegevens alleen plaatsvindt voor zover dat noodzakelijk is voor de goede taakuitoefening door de betreffende ambtenaar. Ten aanzien van de bevoegdheden, die zijn geregeld in de artikelen 33 tot en met 35, geldt om kennis te nemen van de inhoud van telecommunicatie een aparte, met meer waarborgen omklede regeling. Deze regeling houdt in dat alleen door de minister aangewezen ambtenaren die aan hem ondergeschikt zijn (dus geen ambtenaren die overeenkomstig artikel 79 en 80 zijn aangewezen) kennis mogen nemen van de hier bedoelde informatie voor het doel van de desbetreffende bevoegdheidsuitoefening (artikel 33, vierde lid, 34, vijfde lid en 35, vijfde lid). De minister kan de bevoegdheid mandateren aan het hoofd van de dienst. Deze bepalingen dragen niet alleen bij aan de kwaliteit van de wetgeving waaraan nationale wetgeving ingevolge de jurisprudentie van het EHRM in het licht van de voorzienbaarheid moet voldoen, maar zij zijn eveneens van belang in het kader van de vraag naar de proportionaliteit van de inzet van bevoegdheden (zie hieronder).

[164] Een dergelijke overweging heeft het EHRM toegestaan, zie EHRM 18 mei 2010, *Kennedy e.a. t. Verenigd Koninkrijk*, par. 161.

Voor het onderzoeken en opslaan van celmateriaal en het opslaan van DNA-profielen gelden ingevolge artikel 28 van het wetsvoorstel aparte, strikte normen omtrent doelbinding, toestemming en duur en wijze van bewaren. In de Wiv 2002 werd de bevoegdheid om DNA-onderzoek te verrichten begrepen onder de bevoegdheid om onderzoek te verrichten van besloten plaatsen en gesloten voorwerpen (artikel 22, eerste lid, aanhef en onder c, Wiv 2002). In navolging van de jurisprudentie van het EHRM[165] en de aanbevelingen van de CTIVD[166], is ervoor gekozen om de bevoegdheid tot DNA-onderzoek in een aparte bepaling neer te leggen. Het EHRM vereist immers ten aanzien van DNA-onderzoek, net als voor telefoontaps, *'secret surveillance'* en heimelijke informatieverzameling, dat er in de wet gedetailleerde regels worden neergelegd met betrekking tot de reikwijdte en de toepassing van de bevoegdheid. Daartoe dienen in de wet waarborgen te worden gesteld met betrekking tot de duur van de opslag, het gebruik van het materiaal, toegang door derden, procedures om de integriteit en de vertrouwelijkheid van de gegevens te garanderen en procedures met betrekking tot de vernietiging. In artikel 28 van het wetsvoorstel is daaraan gevolg gegeven. De bevoegdheid om op basis van celmateriaal op voorwerpen DNA-onderzoek te verrichten geldt slechts met betrekking tot de vaststelling van de identiteit, waaronder ook verificatie van de identiteit moet worden begrepen. Toestemming kan vanwege het inbreukmakende karakter alleen door de betrokken minister worden verleend. Voorts worden in artikel 28 regels gesteld met betrekking tot doelbinding, verwerking, bewaartermijn en vernietiging van het celmateriaal en de daaruit verkregen gegevens. De bewaartermijn van celmateriaal is zo kort mogelijk gehouden (maximaal drie maanden), conform de overweging van het EHRM in het arrest S. en Marper t. het Verenigd Koninkrijk dat het bewaren van celmateriaal – dat immers informatie kan geven over de genetische afkomst en de gezondheid van de persoon van wie het celmateriaal afkomstig is – in bijzondere mate inbreuk maakt op het recht op bescherming van de persoonlijke levenssfeer van de persoon die het betreft[167]. Bij algemene maatregel van bestuur kunnen daartoe nadere regels worden gesteld, onder andere met betrekking tot de inrichting, het beheer en de toegang tot de DNA-profielen. Met deze bepaling en de nadere regelgeving wordt voldaan aan het vereiste van het EHRM dat de bevoegdheid tot DNA-onderzoek in voldoende detail in de wet is omschreven, waarbij tevens is voorzien in waarborgen tegen misbruik en willekeur.

De hierboven genoemde regels en vereisten tezamen vormen, in samenhang met de eisen omtrent noodzakelijkheid, proportionaliteit en subsidiariteit en de

[165] EHRM 4 november 2008, *S. en Marper t. Verenigd Koninkrijk*, par. 99.
[166] CTIVD toezichtsrapport nr. 42, inzake de toepassing van biologisch forensische onderzoeksmethoden door de AIVD, 7 januari 2005.
[167] EHRM 4 november 2008, *S. en Marper t. Verenigd Koninkrijk*, par. 120 en 121.

toetsingsmogelijkheden (waarover hieronder meer), een divers en ruim scala aan waarborgen tegen misbruik, waarbij voor de zwaarste inbreuken, zoals door DNA-onderzoek, zeer uitvoerige procedurele en andere waarborgen zijn voorzien. Door het totaal aan waarborgen komt de balans tot uiting die in het wetsvoorstel is neergelegd tussen een effectieve bescherming van de nationale veiligheid en de bescherming van de persoonlijke levenssfeer van burgers.

Legitiem doel

Artikel 8 EVRM vereist dat met de beperking een legitiem doel wordt nagestreefd. Het tweede lid van artikel 8 geeft een limitatieve opsomming van de legitieme doelen waarvoor een beperking kan worden ingezet. Het belang van de nationale veiligheid is er een van.

Noodzakelijk in een democratische samenleving

Artikel 8 EVRM vereist ook dat beperkingen noodzakelijk zijn in een democratische samenleving. Dit houdt in dat voor de inbreuk op het recht op eerbiediging van het privéleven een dringend maatschappelijk belang aanwezig is, dat de verwerking van gegevens in een evenredige verhouding staat tot het doel dat ermee wordt nagestreefd, dat de beperking effectief bijdraagt aan de verwezenlijking van het doel en dat er geen minder ingrijpende maar even effectieve, alternatieve middelen bestaan om het doel te bereiken.

Sinds het arrest Klass en anderen t. Duitsland[168] uit 1978 neemt het EHRM aan dat er in democratische samenlevingen een dringend maatschappelijk belang bestaat bij het toestaan van '*secret surveillance*' ten behoeve van de bescherming van de nationale veiligheid.

De staat heeft volgens vaste jurisprudentie van het EHRM een redelijk ruime discretionaire bevoegdheid om te bepalen hoe de nationale veiligheid het best kan worden beschermd. Daarbij moet het belang van de staat worden afgewogen tegen het recht op privacy van haar burgers[169]. De bevoegdheid van de staat om '*secret surveillance'* in te zetten, strekt slechts tot wat strikt noodzakelijk is voor de bescherming van de nationale veiligheid. Dat betekent dat moet worden beoordeeld of er geen minder inbreukmakend middel voorhanden is dat even effectief is. En dat er is voorzien in toereikende en effectieve waarborgen tegen misbruik van bevoegdheden, die zwaarder

[168] EHRM 6 september 1978, *Klass e.a. t. Duitsland*, par. 48
[169] EHRM 26 maart 1987, *Leander t. Zweden*, par. 59.

moeten zijn naarmate een bevoegdheid meer inbreuk maakt op de persoonlijke levenssfeer[170].

In de Wiv 2002 en in het wetsvoorstel is op diverse plekken voorzien in een toets van de noodzakelijkheid, proportionaliteit en subsidiariteit. Ingevolge artikel 17 van het wetsvoorstel vindt de verwerking van gegevens slechts plaats voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van deze wet of de Wet veiligheidsonderzoeken (eerste lid). Ook artikel 23 van het wetsvoorstel, waarin de inzet van bijzondere bevoegdheden wordt beperkt tot bepaalde taken van de diensten, kent een noodzakelijkheidstoets: een bevoegdheid als bedoeld in paragraaf 3.2.2 van het wetsvoorstel mag immers slechts worden uitgeoefend voor zover dat noodzakelijk is voor de goede uitvoering van de daarna genoemde taken van de diensten. Voorts dient in het verzoek om toestemming voor de uitoefening van een bijzondere bevoegdheid altijd het doel en de noodzakelijkheid (waaronder de evenredigheid en subsidiariteit) van de inzet van die bevoegdheid te worden aangegeven. Ten slotte zorgt het afwegingskader dat is neergelegd in de artikelen 43 en 44 van het wetsvoorstel ervoor dat voorafgaand aan elke inzet van een bijzondere bevoegdheid, een belangenafweging wordt gemaakt tussen het belang van de overheid (in casu de zorg voor de nationale veiligheid) en het belang van de betrokkene (in het bijzonder de bescherming van diens persoonlijke levenssfeer). Daarbij moet worden beoordeeld (artikel 43, tweede lid) welke bevoegdheid, gelet op de omstandigheden van het geval waaronder de ernst van de bedreiging van de door een dienst te beschermen belangen, het minste nadeel oplevert voor de betrokkene (subsidiariteitstoets). Dat betekent bijvoorbeeld dat de diensten eerst gebruik moeten maken van de minst inbreukmakende bevoegdheid en dat zij pas daarna, indien dat noodzakelijk blijkt, over mogen gaan tot de inzet van een meer inbreukmakende bevoegdheid[171]. Ook moet in het kader daarvan worden beoordeeld (artikel 43, derde lid) of de uitoefening van de bevoegdheid voor de betrokkene een onevenredig nadeel oplevert in vergelijking met het daarbij na te streven doel (proportionaliteitstoets). In dat geval dient de uitoefening van de bevoegdheid achterwege te blijven. Ook de bepaling (in artikel 44) dat de uitoefening van de bevoegdheid onmiddellijk wordt gestaakt als het doel waartoe de bevoegdheid is ingezet is bereikt of als met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan, is relevant in het kader van de noodzakelijkheid en subsidiariteit die bij belangenafweging moeten worden betrokken.

Bij de beoordeling of is voorzien in toereikende en effectieve waarborgen tegen misbruik kijkt het EHRM naar alle omstandigheden van het geval. Daaronder vallen de aard, de

[170] EHRM 18 mei 2010, *Kennedy t. Verenigd Koninkrijk*, par. 153, EHRM 3 juli 2012, *Robathin t. Oostenrijk*, par. 47-51.
[171] CTIVD rapport nr. 38, p. 56.

reikwijdte en de duur van de (mogelijke) bevoegdheden, de gronden waarop deze kunnen worden ingezet, de autoriteiten die bevoegd zijn om daarvoor toestemming te verlenen en om de bevoegdheden uit te oefenen, het toezicht op de uitvoering en het soort rechtsmiddel dat is voorzien[172].

Tot de waarborgen tegen misbruik die in het wetsvoorstel zijn neergelegd, behoort hetgeen hierboven in het kader van de voorzienbaarheid is uiteengezet over de taken van de inlichtingen- en veiligheidsdiensten, de uitvoerige regeling in het wetsvoorstel van de algemene en bijzondere bevoegdheden die in het kader daarvan kunnen worden ingezet, de daarbij te maken afwegingen, de instanties die toestemming moeten verlenen, de duur van de toestemming, de regelingen ten aanzien van het verwerken, bewaren, verstrekken en vernietigen van persoonsgegevens en de jaarlijkse openbare verslaglegging aan het parlement over de ontplooide en voorgenomen activiteiten van de diensten. Bij de klachtenregeling en andere rechtsmiddelen die burgers ter beschikking staan, wordt in paragraaf 9.3 stilgestaan.

Toezicht

Een andere belangrijke waarborg tegen misbruik is een systeem van toezicht. Het EHRM heeft een voorkeur voor een voorafgaande rechterlijke toets, maar een systeem van toezicht achteraf door een effectieve, onafhankelijke instantie is ook in overeenstemming met het EVRM[173]. Uit de analyse die de commissie Dessens heeft gemaakt van de diverse mogelijkheden van toezicht, volgt ook dat niet met stelligheid is te zeggen dat preventief rechterlijk toezicht effectiever is dan toezicht achteraf. Het EHRM beoordeelt het systeem van waarborgen en bevoegdheden voorts in zijn geheel: het neemt de gehele procedure in beschouwing, waaronder ook alle hierboven opgesomde waarborgen tegen misbruik.

In de huidige wet is voorzien in een systeem van toezicht achteraf door een onafhankelijke en gespecialiseerde toezichthouder, de CTIVD, behalve voor inbreuken op het briefgeheim, waarvoor voorafgaande toestemming nodig is door de rechter. Diverse andere Europese landen kennen een vergelijkbaar stelsel van toezicht. De Commissie Dessens is uitvoerig ingegaan op het systeem van toezicht[174]. Zij komt – mede gelet op de jurisprudentie van het EHRM – tot de aanbeveling om in de Wiv 2002 een

[172] EHRM 6 september 1978, *Klass e.a. t. Duitsland*, par. 50; EHRM 29 juni 2006, *Weber en Saravia t. Duitsland*, par. 106; EHRM 18 mei 2010, *Kennedy t. Verenigd Koninkrijk*, par. 153.
[173] EHRM 6 september 1978, *Klass e.a. t. Duitsland*, par. 55- 56 en EHRM 18 mei 2010, *Kennedy t. Verenigd Koninkrijk*, par. 167
[174] Rapport van de commissie Dessens, Paragraaf 5.5 Extern toezicht op de inzet van bijzondere bevoegdheden.

onafhankelijk, juridisch bindend oordeel te introduceren. Dat zou de vorm moeten krijgen van een bindend rechtmatigheidsoordeel van de CTIVD in combinatie met een onmiddellijke toets[175].

De regering volgt de aanbeveling van de commissie Dessens niet. Dit is eerder ook al aangegeven in de brief van de Minister van BZK van 11 maart 2014 met daarin de kabinetsreactie op het rapport van de commissie Dessens[176] alsmede in het Algemeen Overleg dat hierover op 16 april 2014 is gevoerd[177]. De regering stelt in het wetsvoorstel voor om de positie van de CTIVD anderszins te versterken. Deze regeling voldoet ook aan de vereisten van het EHRM; het gaat het EHRM er immers om dat de toezichthouder daadwerkelijk effectief toezicht kan houden. Daartoe wordt de CTIVD ingevolge het wetsvoorstel verder versterkt. De CTIVD had in het kader van haar taak als toezichthouder al verregaande bevoegdheden toegekend gekregen in de Wiv 2002, waaronder (zelfstandige) toegang tot alle gegevens bij de diensten, verplichte medewerking en de mogelijkheid om personen als getuige of deskundige op te roepen. Deze bevoegdheden worden nog verder versterkt. De versterking bestaat uit de invoering van een meldingsmogelijkheid en een heroverwegingsplicht. De meldingsmogelijkheid houdt in dat de CTIVD de betrokken minister – desgewenst onmiddellijk – kan mededelen dat zij een verleende toestemming voor de uitoefening van een bijzondere bevoegdheid onrechtmatig acht (artikel 102 , eerste lid). Om te voorkomen dat de verantwoordelijke minister al te lichtvaardig over een dergelijk onrechtmatigheidsoordeel van de CTIVD heen zou kunnen stappen, wordt in de wet aan de minister de plicht opgelegd om de door hem verleende toestemming aan een heroverweging te onderwerpen (artikel 102, tweede lid). Indien de minister van oordeel blijft dat de toestemming naar zijn oordeel wel rechtmatig is verleend, dient hij zowel de CTIVD als de CIVD onverwijld daaromtrent te informeren (artikel 102, derde lid). De CIVD – en daarmee dus de Tweede Kamer - kan waar zij dat dienstig acht de minister daarover vervolgens ter verantwoording roepen.

Het is in dit kader voorts van belang de door het kabinet voorgestelde aanpassing van het klachtstelsel te betrekken, waarbij de CTIVD als een (zelfstandige) onafhankelijke klachtinstantie wordt gepositioneerd en die daarbij de bevoegdheid krijgt om jegens de minister bindende oordelen te geven. In paragraaf 7.2.3 van het wetsvoorstel is dit nader uitgewerkt. Hierop wordt nader ingegaan in paragraaf 9.3. Ten slotte is in paragraaf 7.2.4 een klokkenluidersregeling opgenomen voor personen die betrokken zijn bij de

[175] Rapport van de commissie Dessens, pag. 100 – 102.
[176] Kamerstukken II 2013/14, 33 820, nr. 2.
[177] Kamerstukken II 2013/14, 33 820 nr. 3.

uitvoering van deze wet en de Wet veiligheidsonderzoeken en die een vermoeden van een misstand willen melden.

Door dit samenspel van maatregelen wordt op adequate wijze invulling gegeven aan de eisen met betrekking tot waarborgen tegen misbruik die voortvloeien uit artikel 8 EVRM en de daarop betrekking hebbende jurisprudentie van het EHRM.

9.2.2 Het recht op bescherming van persoonsgegevens

In artikel 10 van de Grondwet is niet alleen het recht op eerbiediging van de persoonlijke levenssfeer opgenomen, maar ook, in het tweede lid, een expliciete regelingsopdracht gegeven aan de overheid om regels te stellen ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. In het derde lid van artikel 10 van de Grondwet is de regelingsopdracht neergelegd regels te stellen inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van deze gegevens. Artikel 8 EVRM kent geen expliciete bescherming van persoonsgegevens, maar persoonsgegevens vallen wel onder de reikwijdte van die bepaling, aangezien zij de kern uitmaken van de gegevens die worden beschermd door het recht op eerbiediging van het privéleven. Het hierboven geschetste toetsingskader dat volgt uit het EVRM en de jurisprudentie van het EHRM is dan ook op de verwerking van persoonsgegevens van toepassing.

Zoals hierboven in paragraaf 9.2.1 reeds genoemd, bevat het wetsvoorstel, en met name hoofdstuk 3, een uitgebreide regeling met betrekking tot de bevoegdheden van de inlichtingen- en veiligheidsdiensten tot het verwerken van persoonsgegevens, waaronder regels omtrent het verwerken, bewaren, verstrekken en vernietigen van die gegevens. In dit licht is onder meer relevant wat is opgenomen in artikel 17 van het wetsvoorstel ten aanzien van de algemene regels omtrent de verwerking van gegevens, waaronder persoonsgegevens: ”De verwerking van gegevens geschiedt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze”(tweede lid). Daaronder valt dat de gegevens worden voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend (lid 3). In hoofdstuk 6 van het wetsvoorstel wordt de samenwerking met andere instanties geregeld. Dat hoofdstuk bevat ook bepalingen over het verstrekken van gegevens aan inlichtingen- en veiligheidsdiensten van andere landen. Met dit stelsel van bepalingen is voldaan aan de regelingsopdracht in artikel 10, tweede lid, van de Grondwet.

In hoofdstuk 5 van het wetsvoorstel is een uitgebreide regeling opgenomen voor de kennisneming van gegevens die door of ten behoeve van de inlichtingen- en

veiligheidsdiensten zijn verwerkt. Het EHRM heeft de mogelijkheid om kennis te nemen van de over een persoon verzamelde gegevens beoordeeld onder artikel 8 EVRM, terwijl het EHRM de mogelijkheid om wijzigingen aan te brengen in die gegevens of ze te laten vernietigen, heeft bezien in het licht van het recht op een daadwerkelijk rechtsmiddel (artikel 13 EVRM). Het EHRM erkent hoe dan ook dat de verdragsstaat een zekere discretionaire bevoegdheid heeft waar het gaat om het inzage- en correctierecht.[178] In het geval van de gegevens die door de inlichtingen- en veiligheidsdiensten worden verzameld en verwerkt, dient rekening te worden gehouden met het bijzondere karakter van de activiteiten van deze diensten. Daarom is in de Wiv 2002 en in het huidige wetsvoorstel een specifieke regeling neergelegd inzake kennisneming en correctie, waarbij is afgezien van het toekennen van een correctierecht. De commissie Dessens heeft in haar advies aandacht besteed aan het inzage- en correctierecht en geadviseerd dat personen die inzage hebben gekregen, gemotiveerd moeten kunnen verzoeken om herstel, aanvulling, verwijdering of vernietiging van gegevens[179]. De regering heeft in reactie op dit advies aangegeven dat artikel 48 van de Wiv 2002 (artikel 65 van het wetsvoorstel) aan degene die ingevolge artikel 47 van de Wiv 2002 (artikel 64 van het wetsvoorstel) kennis heeft genomen van door of ten behoeve van de diensten omtrent hem verwerkte gegevens, daaromtrent een schriftelijke verklaring kan overleggen. Deze verklaring wordt bij de desbetreffende gegevens gevoegd, hetgeen materieel gezien vrijwel geheel overeenkomt met een correctierecht, terwijl dit tegelijkertijd recht doet aan de wettelijke plicht tot bronbescherming. De regeling is dan ook volledig in overeenstemming met de vereisten van het EHRM met betrekking tot het recht op inzage en correctie.

9.2.3 Het recht op bescherming van het huisrecht

Artikel 12 van de Grondwet beschermt tegen ongeoorloofd binnentreden in een woning. Het binnentreden in een woning is alleen geoorloofd in de gevallen bij of krachtens de wet bepaald, door hen die daartoe bij of krachtens de wet zijn aangewezen.

Het huisrecht vormt een nadere uitwerking van het recht op bescherming van de persoonlijke levenssfeer, zoals neergelegd in artikel 10 van de Grondwet. Het huisrecht maakt ook expliciet onderdeel uit van het artikel 8, eerste lid, EVRM: "*Everyone has the right to respect for his private and family life, his home and his correspondence*". De tekst artikel 17 IVBPR is gelijkluidend aan die van artikel 8, eerste lid, EVRM: ook in die bepaling is het huisrecht expliciet erkend.

[178] EHRM 6 juni 2006, *Segerstedt-Wiberg en anderen t. Zweden*, par. 102-104.
[179] Rapport commissie Dessens, pag. 139 e.v.

Het huisrecht is, net als het algemenere recht op bescherming van de persoonlijke levenssfeer, niet absoluut en kan aan beperkingen worden onderworpen. In artikel 12, eerste lid, van de Grondwet is bepaald dat het binnentreden in een woning zonder toestemming van de bewoner alleen is geoorloofd in de gevallen bij of krachtens de wet bepaald, door hen die daartoe bij of krachtens de wet zijn aangewezen. Daarnaast gelden ingevolge het tweede en derde lid van artikel 12 een aantal vormvereisten die verbonden zijn aan het binnentreden in een woning (voorafgaande legitimatie en mededelen van het doel van het binnentreden en notificatie achteraf). Met name in het derde lid is rekening gehouden met het feit dat het belang van de nationale veiligheid onder omstandigheden zich tegen notificatie kan verzetten; er is zowel voorzien in de mogelijkheid van uitstel als afstel van de notificatie. Artikel 27 van het wetsvoorstel, waarin de bevoegdheid is neergelegd om besloten plaatsen te doorzoeken; artikel 42 van het wetsvoorstel, waarin een accessoire bevoegdheid is neergelegd tot toegang tot woningen en de Algemene wet op het binnentreden geven gezamenlijk uitwerking aan deze grondwettelijke vereisten. Daarnaast wordt voldaan aan alle vereisten die artikel 8 EVRM aan deze bevoegdheid stelt: er is een basis in de wet, de bepalingen zijn voldoende nauwkeurig omschreven, de bovengenoemde waarborgen tegen misbruik – zoals de toestemmingsregeling – zijn van toepassing op de bevoegdheid tot binnentreden in de woning, evenals de genoemde bepalingen omtrent een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging.

Resumerend stellen wij vast dat de in het wetsvoorstel opgenomen regeling inzake het binnentreden van een woning zonder toestemming van de bewoner voldoet aan de eisen van artikel 12 Grondwet en artikel 8 EVRM.

9.2.4 Het recht op bescherming van het brief-, telefoon- en telegraafgeheim

Artikel 13 van de Grondwet beschermt het brief-, telefoon- en telegraafgeheim. Dit artikel vormt, net als het hiervoor besproken artikel 12 van de Grondwet, een uitwerking van een specifiek aspect van het algemene recht op bescherming van de persoonlijke levenssfeer dat wordt beschermd door artikel 10 van de Grondwet. Artikel 13 van de Grondwet is door de enorme ontwikkelingen op het gebied van elektronische communicatie in de afgelopen decennia, al enige tijd achterhaald. Recent is door de regering een voorstel tot wijziging van artikel 13 ingediend[180]. Dit voorstel is nog niet door het parlement aanvaard. Niettemin zal in deze paragraaf waar relevant kort worden ingegaan op de voorgestelde wijzigingen en de gevolgen daarvan voor de in dit wetsvoorstel gewijzigde stelsel van interceptiebevoegdheden.

[180] Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepaling inzake de onschendbaarheid van het brief- telefoon- en telegraafgeheim, 22 juli 2014, Kamerstukken II 2013/14, 33 989.

Artikel 13 van de Grondwet stelt verschillende vereisten aan inbreuken op enerzijds het briefgeheim en anderzijds het telefoon- en telegraafgeheim. Voor inbreuken op het briefgeheim vereist artikel 13, eerste lid, dat deze een basis hebben in een wet in formele zin en dat daarvoor vooraf toestemming wordt verleend door de rechter. Voor inbreuken op het telefoon- en telegraafgeheim in het belang van de nationale veiligheid vereist artikel 13, tweede lid, van de Grondwet dat deze een basis hebben in een formele wet of in lagere regelgeving en dat een inbreuk slechts kan worden gemaakt door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Artikel 8 EVRM is niet alleen van toepassing op het brief-, telefoon- en telegraafgeheim, maar ook op inhoud van communicatie die via andere communicatiemiddelen wordt getransporteerd. Het thans aanhangig zijnde herzieningsvoorstel voor artikel 13 Grondwet stelt voor alle inhoud van communicatie, ongeacht met welk communicatiemiddel deze wordt overgebracht, aan dezelfde eisen te onderwerpen. Artikel 8 EVRM kent een hiermee vergelijkbare benadering. Artikel 8 EVRM vereist daarnaast dat een inbreuk op het in artikel 8 EVRM neergelegde recht een legitiem doel moet dienen, bij wet moet zijn voorzien en noodzakelijk moet zijn in een democratische samenleving.

Wat is beschermd?

Artikel 13 van de Grondwet en artikel 8 EVRM beschermen het recht op gerichte, niet openbare communicatie, ofwel privécommunicatie. De vertrouwelijkheid van communicatie tussen twee of meer personen, instellingen of organisaties vormt in een democratische rechtsstaat een zwaarwegend belang[181]. Privécommunicatie moet, gelet op het niet-openbare karakter van de inhoud derhalve worden beschermd tegen heimelijke onderschepping door de overheid. Het recht op bescherming van de privécommunicatie geldt niet voor communicatie die openbaar is. Dergelijke communicatie, zoals het posten van berichten op een website die voor het brede publiek toegankelijk zijn, valt daar niet onder omdat deze communicatie bewust is opengesteld voor of bekendgemaakt aan eenieder. Deze openbare communicatie wordt beschermd door het recht op vrijheid van meningsuiting zoals dat is neergelegd in artikel 7 van de Grondwet en artikel 10 van het EVRM. Privécommunicatie omvat ook communicatie aan groepen personen zoals nieuwsbrieven, of binnen groepen personen zoals chats op een alleen voor leden toegankelijke website[182].

Artikel 13 van de Grondwet ziet alleen op communicatie door middel van een communicatiemiddel waarbij een derde belast is met het transport – en in het voorgestelde gewijzigde artikel 13 van de Grondwet ook met de opslag. Daarbij kan

[181] Kamerstukken 2013/14, 33 989, nr. 3, blz. 8.
[182] Kamerstukken 2013/14, 33 989. Nr. 3, blz. 15-17.

worden gedacht aan het transport van brieven door aanbieders van postbezorging (aanbieders in de zin van de Postwet 2009 en aanbieders van private koeriersdiensten), maar ook aan het transport van e-mailverkeer of mobiele telefonie door aanbieders van elektronische communicatiediensten. Zogenaamde onmiddellijke communicatie – waarbij geen communicatiemiddel wordt gebruikt – valt derhalve niet onder de bescherming van artikel 13 van de Grondwet. Daarbij is vooral het live gesprek van belang. Deze communicatievorm wordt beschermd onder artikel 10 van de Grondwet.

De bescherming van artikel 13 van de Grondwet betreft voorts slechts de inhoud van de communicatie. Verkeersgegevens ofwel metadata, die geen informatie geven over de inhoud maar slechts over de overdracht en de opslag van de communicatie, vallen buiten het bereik van artikel 13. Deze gegevens worden wel beschermd door artikel 10 van de Grondwet en artikel 8 EVRM[183]. Zij kunnen immers informatie geven over het privéleven van de betrokkene, zoals over diens communicatiepatroon en degenen met wie hij in contact staat. Het EHRM liet in haar uitspraken hierover in het midden of deze gegevens worden beschermd door het algemene recht op privéleven of door het communicatiegeheim – de bescherming is in beide gevallen hetzelfde. In de praktijk blijkt het vaak lastig om verkeersgegevens en inhoud te scheiden. Bijvoorbeeld omdat de onderwerpregel van e-mails informatie geeft over de inhoud van de communicatie. In die gevallen waarin de verkeersgegevens de inhoud van de communicatie betreffen, vallen deze gegevens wel onder de reikwijdte van artikel 13 van de Grondwet.

Bescherming briefgeheim

Artikel 29 van het wetsvoorstel voorziet in een bevoegdheid tot het maken van een inbreuk op het briefgeheim. In deze bepaling wordt uitvoering gegeven aan het grondwettelijke vereiste dat voor een dergelijke inbreuk voorafgaande, rechterlijke machtiging is vereist (artikel 29, eerste lid).

De door de regering voorgestelde wijziging van artikel 13 van de Grondwet laat ruimte voor een afwijkende regeling. Immers, in de hoofdregel is de eis van een voorafgaande rechterlijke machtiging weliswaar opgetrokken naar alle vormen van telecommunicatie, inclusief communicatie per post, maar daarin is ook voorzien in een uitzondering op dat vereiste voor de nationale veiligheid. Aangezien dit wetsvoorstel thans nog ter behandeling in de Staten-Generaal voorligt, zijn de eventuele gevolgen van de voorgestelde wijziging voor deze bevoegdheid van de diensten op dit moment niet aan de orde. Het onderhavige wetsvoorstel voldoet dan ook aan de thans geldende

[183] Zie onder meer EHRM 2 augustus 1984, *Malone t. Verenigd Koninkrijk*, par. 84, EHRM 25 september 2001, *P.G. en J.H. t. het Verenigd Koninkrijk*, par. 42.

grondwettelijke eis van een voorafgaande rechterlijke machtiging. In zoverre is geen verandering beoogd met de waarborgen die in de Wiv 2002 zijn neergelegd.

In het kader van waarborgen tegen misbruik is nog relevant dat de algemene regeling in artikel 46 van het wetsvoorstel inzake notificatie van toepassing is op de bevoegdheid tot het openen van correspondentie. Op basis daarvan dient er verslag te worden gedaan aan de betrokkene van de inbreuk op het briefgeheim, tenzij gronden aanwezig zijn voor uitstel of afstel daarvan.

Bescherming telecommunicatie

Artikel 13 van de Grondwet beschermt op dit moment naast correspondentie per post, alleen het telefoon- en telegraafverkeer. De voorgestelde wijziging van artikel 13 van de Grondwet trekt de bescherming daarvan op tot alle huidige en toekomstige telecommunicatiemiddelen. Op dit moment zijn de meeste huidige communicatiemiddelen al beschermd door artikel 8 EVRM, aangezien de begrippen 'private life' en 'correspondence' door het EHRM steeds ruim zijn uitgelegd. De jurisprudentie van het EHRM ziet tot nu toe op bescherming van communicatie per brief, telefoon[184] en e-mail, zowel thuis[185] als op het werk[186], maar ook op bescherming tegen het volgen van een persoon via GPS[187], het verzamelen van publieke informatie over een persoon[188], het aftappen van pager berichten[189] en het via de media bekend maken van beelden op bewakingscamera's[190].

Het recht op bescherming van de telecommunicatie is aan de orde bij de artikelen van paragraaf 3.2.2.7 van het wetsvoorstel, dat ziet op onderzoek naar de inhoud van communicatie. Het gaat meer concreet om de bevoegdheden tot interceptie van communicatie (artikel 32 en 33), het searchen (artikel 34) en selecteren van de gegevens (artikel 35) die door middel van de interceptie ex artikel 33 zijn verkregen. De jurisprudentie van het EHRM is op al deze vormen van verwerking van gegevens van toepassing[191].

Artikel 13 van de Grondwet geeft voor wat betreft inzage in het belang van de nationale veiligheid geen bijzondere vereisten voor inbreuken op het telefoon- en telegraafgeheim, anders dan dat deze moeten zijn voorzien bij wet en dat de inbreuken uitsluitend mogen

[184] EHRM 6 september 1978, *Klass t. Duitsland*, par. 41.
[185] *Kruslin t. Frankrijk, Huvig t. Frankrijk*
[186] EHRM 25 juni 1997, *Halford t Verenigd* Koninkrijk; EHRM 3 juli 2007, *Copland t. Verenigd Koninkrijk*.
[187] EHRM 2 september 2010, *Uzun t. Duitsland*
[188] EHRM 25 mei 2011, *Association "21 Decembre 1989" en anderen t. Roemenië*.
[189] EHRM 22 oktober 2002, *Taylor – Sabori t. Verenigd Koninkrijk*, nr. 47114/99.
[190] EHRM 28 januari 2003, *Peck t. Verenigd Koninkrijk*.
[191] Zie ook CTIVD rapport nr. 38, p. 47-48.

worden uitgevoerd door hen die daartoe bij of krachtens de wet zijn aangewezen. Artikel 8 EVRM beschermt de telecommunicatie op dezelfde wijze als andere inbreuken op de persoonlijke levenssfeer, middels het hierboven uiteengezette toetsingskader. Voor zover gerichte interceptie betrekking heeft op 'live' gesprekken, is artikel 10 van de Grondwet van toepassing. Dit artikel stelt echter, in relatie tot de bescherming van 'live' gesprekken, geen nadere eisen aan de uitoefening van de bevoegdheid zoals artikel 13 van de Grondwet wel doet.

De bepalingen in paragraaf 3.2.2.7 van het wetsvoorstel voldoen aan alle eisen die artikel 13 van de Grondwet en artikel 8 EVRM daaraan stellen.

Waarborgen rondom interceptie van de inhoud van communicatie

Daarnaast zijn deze bevoegdheden ruimschoots van de nodige waarborgen voorzien. Daar is voor gekozen omdat het onderzoek van communicatiegegevens een belangrijke rol speelt in de taken van de diensten, maar het verzamelen van gegevens over communicatie en het verwerken van die gegevens vrijwel altijd een inbreuk maakt op de persoonlijke levenssfeer van burgers (een uitzondering is militair verkeer, zie de uitzondering van artikel 32, negende lid). Alle algemene waarborgen tegen misbruik die zijn opgenomen in de bepalingen over de verwerking en verzameling van (persoons)gegevens en de verstrekking van gegevens door de diensten zijn op de bepalingen omtrent onderzoek van communicatie van toepassing, evenals alle hierboven besproken algemene bepalingen die invulling geven aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Ook hetgeen hierboven is gesteld omtrent toezicht en ministeriële verantwoordelijkheid is op deze bepalingen van toepassing. Daarnaast gelden ten aanzien van deze bevoegdheden nog diverse aanvullende waarborgen, die zwaarder worden naar gelang de mate van inbreuk op het privéleven. Voor interceptie, search en selectie is toestemming voorafgaand aan de inbreuk van de minister nodig, wat volgens het EHRM een belangrijke waarborg vormt tegen misbruik[192]. Deze toestemmingsbevoegdheid kan niet worden gedelegeerd of gemandateerd. Ook het stellen van limieten aan de bewaartermijnen van gegevens is een volgens de jurisprudentie van het EHRM belangrijke waarborg[193]. Dit heeft uitwerking gekregen in de opdracht om door middel van gerichte interceptie verworven gegevens zo snel mogelijk te onderzoeken op hun relevantie voor het onderzoek waarvoor ze zijn verworven ten behoeve waarvan de gegevens ten hoogste twaalf maanden mogen worden bewaard, waarna niet relevante gegevens of gegevens die niet op hun relevantie zijn onderzocht dienen te worden vernietigd (artikel 32, tiende lid) alsmede een

[192] EHRM 29 juni 2006, *Weber en Saravia t. Duitsland*, par. 95.
[193] EHRM 29 juni 2006, *Weber en Saravia t. Duitsland*, par. 95, EHRM 4 mei 2000, *Rotaru t. Roemenië*, par. 57, EHRM 24 mei 2011, *Association "21 Decembre 1989",* par. 169-172.

vergelijkbare regeling voor de (ontsleutelde) gegevens die zijn verworven door uitoefening van de interceptiebevoegdheid van artikel 33, met dien verstande dat daar de termijn op drie jaar is gesteld (artikel 33, vijfde lid). Ook de regelingen voor kennisname van de gegevens (artikelen 33, vierde lid, 34, vijfde lid, en 35, vijfde lid van het wetsvoorstel) geven uitvoering aan het vereiste van het EHRM dat de bevoegdheden met voldoende waarborgen tegen misbruik moeten zijn omkleed[194]. Ten aanzien van de waarborgen tegen misbruik bij gerichte interceptie is nog relevant om te wijzen op artikel 32, vierde lid, van het wetsvoorstel, waarin de procedure is neergelegd in gevallen waarin bij het verzoek om toestemming het nummer nog niet bekend is. In dat geval wordt de toestemming slechts verleend onder de voorwaarde dat de bevoegdheid slechts mag worden uitgeoefend zodra het nummer bekend is. De diensten mogen onderzoek doen ter vaststelling van het nummer, maar alle gegevens die zij daarbij ontvangen die geen betrekking hebben op (het achterhalen van) het nummer, moeten terstond vernietigd worden. Dit draagt bij aan de proportionaliteit van de inzet van deze bevoegdheid[195]. Met betrekking tot de selectie is nog relevant te vermelden dat in dat artikel uitdrukking is gegeven aan de noodzakelijkheidstoets doordat de criteria op basis waarvan de gegevens worden geselecteerd, moeten zijn voorzien van een toereikende motivering in relatie tot het onderzoek waarvoor de selectie dient te worden toegepast.

De hierboven besproken waarborgen, in samenhang met de algemene waarborgen die in het wetsvoorstel zijn vervat en die hierboven in paragraaf 9.2.1 zijn besproken, leiden tot de conclusie dat het stelsel van interceptiebevoegdheden in het wetsvoorstel voorzien is van voldoende maatregelen die tot doel hebben de uitoefening van deze bevoegdheden te limiteren en reguleren teneinde met het oog op de bescherming van de persoonlijke levenssfeer van de burger. Daarmee voldoen de bepalingen omtrent de bevoegdheden tot onderzoek van communicatie aan de eisen die de Grondwet en het EHRM daaraan stellen.

9.3 Het recht op een daadwerkelijk rechtsmiddel

Artikel 13 van het EVRM garandeert het recht op een daadwerkelijk rechtsmiddel (*effective remedy*). Dat betekent dat eenieder die meent dat zijn rechten, zoals gewaarborgd door het EVRM, door de staat zijn of worden geschonden, daarover een klacht moet kunnen indienen bij een bevoegde nationale autoriteit. Deze autoriteit moet niet alleen bevoegd zijn om de klacht inhoudelijk te behandelen, maar ook om passend

[194] EHRM 29 juni 2006, *Weber en Saravia t. Duitsland*, par. 95 en 17 december 1999, *B.B. t. Frankrijk* en *Gordel t. Frankrijk*.
[195] EHRM 3 juli 2012, *Robathin t. Oostenrijk*, par. 47-51.

herstel te bieden[196]. De staat heeft enige beleidsvrijheid ten aanzien van de aanwijzing van een nationale autoriteit en de organisatie van het klachtrecht, maar de voorziening die de staat treft moet beschikbaar en afdoende zijn[197] en effectief, zowel rechtens als in de praktijk[198]. De nationale autoriteit hoeft volgens de jurisprudentie van het EHRM geen rechterlijke instantie te zijn. Het EHRM beoordeelt aan de hand van de bevoegdheden van de autoriteit en de procedurele waarborgen of sprake is van een daadwerkelijk rechtsmiddel. In 2006 heeft het EHRM geoordeeld, in de zaak Segerstedt-Wiberg t. Zweden, dat de autoriteit de bevoegdheid moet bezitten om bindende beslissingen te nemen en om te kunnen bepalen dat verwerkte gegevens worden verwijderd en vernietigd. Eerder al bepaalde het EHRM dat een klager zich direct moet kunnen wenden tot een autoriteit die bevoegd is om de staat op te dragen gegevens over de klager die door de inlichtingen- en veiligheidsdiensten zijn verwerkt, te verwijderen en vernietigen[199]. De mogelijkheid om alleen een klacht in te dienen bij een 'tusseninstantie' die een andere autoriteit om verwijdering of vernietiging kan verzoeken of daartoe kan opdragen, is geen daadwerkelijk rechtsmiddel. Daarnaast kan uit de zaak Segerstedt-Wiberg t. Zweden worden afgeleid dat het van belang is dat de betreffende autoriteit specifiek tot taak heeft om zaken te onderzoeken waarin sprake is van "*secret surveillance*". Een algemeen bevoegde klachteninstantie volstaat dus niet om te kunnen spreken van een daadwerkelijk rechtsmiddel.

Het EHRM beoordeelt de vraag of in een lidstaat sprake is van een daadwerkelijk rechtsmiddel op basis van alle beschikbare voorzieningen gezamenlijk. Dat wil zeggen dat als één van de in een lidstaat aanwezige voorzieningen voor klachtbehandeling niet voldoet aan de hierboven weergegeven eisen, nog niet direct sprake is van een schending van artikel 13 van het EVRM. Pas als het stelsel van voorzieningen in zijn geheel niet voldoet is daarvan sprake[200]. De wijzigingen in het wetsvoorstel ten aanzien van de klachtbehandelingsfunctie van de CTIVD zorgen ervoor dat deze functie van de CTIVD op zichzelf genomen al 'EVRM-proof' is en een daadwerkelijk rechtsmiddel biedt aan burgers. Daarnaast zijn er nog aanvullende rechtsmiddelen beschikbaar.

Naar aanleiding van de ontwikkeling in de jurisprudentie van het EHRM en in navolging van de aanbeveling van de commissie Dessens heeft de regering besloten om de CTIVD

---

[196] EHRM 21 januari 2011, *M.S.S. t. België en Griekenland*, par. 288; EHRM 25 juni 1997, *Halford t. Verenigd Koninkrijk*, par. 64.
[197] Zie ook *Guide to good practice in respect to domestic remedies*, aangenomen door het Comité van Ministers van de Raad van Europa op 18 september 2013, p. 12.
[198] EHRM 13 december 2012, *El-Masri t. "De voormalige Joegoslavische Republiek Macedonie"*, par. 255; EHRM 26 oktober 2000, *Kudła t. Polen*, par. 152.
[199] EHRM 6 juni 2006, *Segerstedt-Wiberg t. Zweden*, par. 117 e.v.
[200] EHRM 13 december 2012, *De Souza Ribeiro t. Frankrijk*, EHRM 26 oktober 2000, par. 79; *Kudła t. Polen*, par. 157.

positioneren als een onafhankelijke klachtbehandelaar. De CTIVD krijgt de bevoegdheid om jegens de minister bindende oordelen te geven over klachten over het optreden of het vermeende optreden van de diensten. De minister is verplicht aan de oordelen van de CTIVD gevolg te geven (artikel 113, vijfde lid, van het wetsvoorstel) en dient bovendien de afdeling klachtbehandeling evenals de klager binnen twee weken te informeren over de wijze waarop aan het oordeel van de afdeling klachtbehandeling uitvoering zal worden gegeven en binnen welke termijn. De CTIVD kan de burger herstel bieden, niet alleen in de vorm van een opdracht tot verwijdering en vernietiging van omtrent de betreffende burger verwerkte gegevens zoals het EHRM eist, maar ook door opdracht te geven tot het staken van een lopend onderzoek of het beëindigen van de uitoefening van een bijzondere bevoegdheid (artikel 113, vierde lid). De mogelijkheid om een klacht in te dienen is laagdrempelig: klachten dienen te voldoen aan een aantal weinig belastende inhoudelijke en vormvoorschriften. De CTIVD ten slotte is gehouden om klachten te beoordelen, tenzij sprake is van een aantal limitatief in artikelen 109, 110 of 111 van het wetsvoorstel opgesomde gevallen, bijvoorbeeld als de klacht over een ander onderwerp gaat dan het (vermeende) optreden van de diensten, als het elk belang ontbeert of kennelijk ongegrond is. Daarmee is gewaarborgd dat de CTIVD niet zonder gewichtige reden kan beslissen om een klacht niet te behandelen.

Met de voorgestelde wijzigingen in het stelsel van voorzieningen voor klachtbehandeling is voorzien in een stevige en tegelijkertijd laagdrempelige klachtbehandelingsautoriteit met kennis van de specifieke context van "*secret surveillance*" en met een ruime bevoegdheid tot het bieden van herstel. Aan alle vereisten die het EHRM stelt aan klachtbehandeling in de context van de nationale veiligheid, wordt hiermee ruimschoots voldaan.

Hoofdstuk 10 Financiële gevolgen voor het Rijk

In het wetsvoorstel wordt in artikel 33 voorzien in de mogelijkheid voor de diensten om in bulk telecommunicatie te intercepteren. Anders dan in het huidige artikel 27 Wiv 2002 is voorzien, zal deze bevoegdheid zich ook gaan uitstrekken tot zogeheten kabelgebonden telecommunicatie. Voor de uitvoering van laatstgenoemde bevoegdheid is voorzien in de medewerking van daarvoor in aanmerking komende aanbieders van communicatiediensten (artikel 37). Waar het gaat om het kostendragerschap is hierbij aansluiting gezocht bij de bestaande wetgeving op het gebied van het tappen, te weten artikel 13.6 Tw. Dat betekent dat de investerings-, exploitatie- en onderhoudskosten met betrekking tot de door die aanbieder te treffen technische voorzieningen in verband met de uitvoering van een ingevolge artikel 33, eerste lid, verleende toestemming, door de desbetreffende aanbieder dienen te worden gedragen (artikel 13.6, eerste lid, Tw). Een

gedetailleerd inzicht in de kosten van interceptie van telecommunicatie op kabelgebonden netwerken als hier bedoeld is op dit ogenblik echter nog niet mogelijk. Deze kosten zullen de komende periode in nauw overleg met relevante aanbieders in de telecomsector in kaart worden gebracht. Het overleg met relevante aanbieders in de telecomsector is tevens vereist om te achterhalen hoe deze bevoegdheid in een technisch complexe omgeving op de meest doeltreffende en doelmatige manier kan worden toegepast, met zo min mogelijk inbreuken op de persoonlijke levenssfeer van burgers. Bij de implementatie van de interceptie van telecommunicatie op kabelgebonden netwerken in het kader van de nieuwe wet is voorts sprake van schaalbaarheid in omvang en tijd. De keuzes die hierbij worden gemaakt hebben vanzelfsprekend gevolgen voor het financiële beslag. Mede om ervaring op te doen op grond waarvan gerichte vervolgstappen kunnen worden genomen, zal de interceptie na inwerkingtreding van de wet in de aanvangsjaren tot enkele fysieke toegangspunten beperkt blijven.

Voorts is een belangrijke voorwaarde voor de modernisering van het interceptiestelsel de intensivering van het toezicht door de Commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten (CTIVD). De CTIVD zal daarvoor in personele zin worden versterkt. De benodigde middelen voor deze intensivering van de CTIVD zullen worden toegevoegd in de Rijksbegroting hoofdstuk III, Algemene Zaken.

Hoofdstuk 11 Lasten voor het bedrijfsleven

In het wetsvoorstel, meer in het bijzonder in paragraaf 3.2.2, waarin een regeling voor de bijzondere bevoegdheden van de diensten wordt getroffen, wordt op enkele onderdelen de medewerking van het bedrijfsleven gevraagd. Het betreft hier medewerking bij het verstrekken van informatie (informatieplicht) alsmede medewerking bij de uitvoering van een verleende toestemming (uitleveren brieven en geadresseerde zendingen, uitvoering toestemming tot interceptie van telecommunicatie, verstrekken van gegevens van gebruikers en ontsleuteling van gegevens). Het verlenen van de gevraagde medewerking brengt voor het bedrijfsleven lasten met zich mee. Deze worden voor een deel door de overheid gecompenseerd.

Medewerking bij de uitlevering van post en andere geadresseerde zendingen

Evenals in de huidige wet is bepaald (artikel 23, zevende lid, Wiv 2002), voorziet artikel 29, zesde lid, van het wetsvoorstel in de verplichting van een instelling van post en vervoer om medewerking te verlenen aan de uitvoering van een door de rechtbank Den Haag afgegeven last, waarbij de diensten toestemming is verleend tot het openen van brieven en andere geadresseerde zendingen. Het gaat daarbij concreet om het uitleveren van de brieven en andere geadresseerde zendingen aan de dienst en deze nadat deze

zijn geretourneerd weer in het reguliere proces van postbezorging op te nemen. De directe kosten die door de instelling van post en vervoer worden gemaakt voor het kunnen voldoen aan de last – in casu de feitelijke uitlevering aan de diensten – komen, evenals dat in het kader van strafvordering het geval is, voor vergoeding in aanmerking.

Medewerking bij de interceptie van telecommunicatie

Het wetsvoorstel breidt de medewerkingsplicht bij de uitvoering van een verleende toestemming tot interceptie van telecommunicatie uit van de aanbieders van openbare telecommunicatienetwerken- en diensten tot de aanbieders van communicatiediensten. Daarnaast wordt de bevoegdheid ook anderszins uitgebreid. De huidige wet kent in artikel 27 de bevoegdheid tot ongerichte interceptie van niet-kabelgebonden telecommunicatie, waarbij niet voorzien is in een medewerkingsplicht voor aanbieders van een openbaar telecommunicatienetwerk of openbare telecommunicatiedienst. In het wetsvoorstel wordt voorzien in een technologieonafhankelijke bevoegdheid tot het in bulk intercepteren van telecommunicatie, waardoor deze zich ook uitstrekt tot het kabelgebonden domein. Deze bevoegdheid wordt bovendien uitgevoerd met medewerking van de desbetreffende aanbieder van een communicatiedienst. Dat betekent dat in het wetsvoorstel de medewerkingsplicht zowel ziet op de bevoegdheid tot gerichte interceptie (artikel 32) als op de bevoegdheid tot interceptie van communicatie in andere gevallen (bulk-interceptie; artikel 33).

Voor de (klassieke) aanbieders van openbare telecommunicatienetwerken en -diensten wordt in hoofdstuk 13 van de Telecommunicatiewet (Tw) zowel aftapbaarheid van hun netwerken en diensten als de medewerkingsplicht bij een toestemming als bedoeld in de Wiv 2002 geregeld tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken worden afgewikkeld onderscheidenlijk tot het aftappen en opnemen van door hen verzorgde telecommunicatie (artikel 13.2, eerste en tweede lid, Tw). Voorts is er een regeling getroffen voor de daarmee samenhangende kosten (artikel 13.6 Tw). Waar het gaat om de aftapbaarheid van hun netwerken en diensten geldt dat ingevolge artikel 13.6, eerste lid, Tw de investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen die door de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn of worden gemaakt teneinde te kunnen voldoen aan (onder meer) artikel 13.1 Tw te hunnen laste komen. In het wetsvoorstel is voor de aanbieders van communicatiediensten, niet zijnde aanbieders van openbare telecommunicatienetwerken en –diensten, de in artikel 13.6, eerste lid, Tw neergelegde regeling, van overeenkomstige toepassing verklaard; artikel 32, achtste lid, en artikel 37, zevende lid, van het wetsvoorstel voorzien daarin. Dat betekent voor de hier bedoelde categorie van aanbieders van communicatiediensten dat

deze zowel voor het kunnen voldoen aan een verleende toestemming tot interceptie ex artikel 32, tweede lid (gericht) als 33, tweede lid (bulk), de daarmee samenhangende kosten voor de te treffen technische voorzieningen door henzelf dienen te worden gedragen; voor de aanbieders van openbare telecommunicatienetwerken en –diensten die worden geconfronteerd met een verzoek om medewerking aan een verleende toestemming ex artikel 33, tweede lid, geldt hetzelfde. Dit laatste is immers ook voor deze aanbieders een nieuwe, op grond van dit wetsvoorstel te introduceren verplichting. Op deze wijze wordt derhalve tussen de te onderscheiden categorieën van aanbieders van communicatiediensten geen verschil gemaakt waar het gaat om de vraag wie de kosten voor deze voorzieningen dient te dragen.

Informatieplicht in verband met de toepassing van artikel 33

In artikel 36, eerste lid, van het wetsvoorstel wordt aan de diensten de bevoegdheid toegekend om zich te wenden tot een aanbieder van een communicatiedienst met het verzoek gegevens te verstrekken, welke noodzakelijk zijn om toepassing te kunnen geven aan de bevoegdheid als bedoeld in artikel 33, eerste lid. In artikel 36, zesde lid, van het wetsvoorstel wordt daarop artikel 13.6, tweede en derde lid, Tw van overeenkomstige toepassing verklaard. Dat betekent dat de door deze aanbieders gemaakte administratiekosten en personeelskosten die rechtstreeks voortvloeien uit het voldoen aan dit verzoek worden vergoed uit ’s-Rijks kas.

Informatieverplichting en medewerkingsplicht met betrekking tot telecommunicatiegegevens

In paragraaf 3.2.2.7.5 van het wetsvoorstel wordt de bevoegdheid voor de diensten geregeld tot het opvragen van bij een aanbieder van communicatiediensten opgeslagen telecommunicatie van een gebruiker als onderdeel van de door hem verleende dienst (artikel 38), het opvragen van verkeersgegevens (artikel 39) en het opvragen van abonneegegevens (artikel 40). In al die gevallen geldt voor de aanbieders een medewerkingsplicht, die – in lijn met hetgeen hiervoor is gesteld met betrekking tot de medewerking bij interceptie – deels zijn regeling vindt in hoofdstuk 13 Tw en deels in onderhavig wetsvoorstel. Dat geldt derhalve ook voor de daarmee samenhangende regeling inzake de kosten. In alle gevallen geldt dat de door de aanbieder gemaakte administratiekosten en personeelskosten die rechtstreeks voortvloeien uit het voldoen aan verzoeken als hier bedoeld worden vergoed uit ’s-Rijks kas. Daartoe is in artikel 38, zesde lid, artikel 13.6, tweede en derde lid, Tw van overeenkomstige toepassing verklaard; in artikel 39, zesde lid, onderscheidenlijk, 40, zevende lid, zijn artikel 13.6, tweede en derde lid, Tw van overeenkomstige toepassing verklaard voor het voldoen aan een verzoek om informatieverstrekking, voor zover deze aanbieders niet reeds op grond

van artikel 13.6, tweede en derde lid, Tw voor vergoeding in aanmerking komen. Voor zover hier relevant, treedt er dus geen wijziging op ten aanzien van de bestaande situatie waar het gaat om de vergoeding van de hier bedoelde kosten.

Medewerkingsplicht met betrekking tot de ontsleuteling van gegevens

In artikel 30 van het wetsvoorstel wordt een regeling getroffen voor de bevoegdheid van de diensten tot het verkennen van en binnendringen in geautomatiseerde werken. In dat kader is ook voorzien in de mogelijkheid voor de diensten om zich tot degene te wenden van wie redelijkerwijs vermoed wordt dat hij kennis draagt van de wijze van versleuteling van de gegevens verwerkt of opgeslagen in het geautomatiseerde werk met het verzoek alle noodzakelijke medewerking te verlenen tot het ontsleutelen van de gegevens door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken (artikel 30, vijfde lid). In artikel 30, achtste lid, is bepaald dat de betrokkene verplicht is aan het verzoek te voldoen. Een vergelijkbare voorziening is in artikel 41 van het wetsvoorstel getroffen waar het gaat om de ontsleuteling van gegevens die door de uitoefening van de bevoegdheid als bedoeld in artikel 32, eerste lid, en 33, eerste lid, zijn verkregen. De hier bedoelde medewerkingsplicht kan zich richten tot individuele burgers, maar evenzeer tot bedrijven. In de huidige wet is ook in een medewerkingsplicht bij ontsleuteling voorzien (zie de artikelen 24, derde lid en 25, zevende lid, Wiv 2002). Voor de daarmee gepaard gaande kosten voor betrokkene is echter geen vergoedingsregeling getroffen. In onderhavig wetsvoorstel wordt deze lijn bestendigd. Eventuele kosten die aan de medewerking verbonden zijn komen aldus te hunnen laste.

Hoofdstuk 12 Consultatie, adviezen en privacy impact assessment

PM

II Artikelsgewijze toelichting

Artikelen 13, 14, 19 en 48

Vanwege de introductie van artikel 80 behoeven enkele andere artikelen, waarin thans al naar artikel 79 wordt verwezen, aanpassing. Voor de ambtenaren die op grond van artikel 80 worden aangewezen komen hierdoor, net als voor de ambtenaren die op grond van artikel 79 zijn aangewezen, regels omtrent het niet al dan niet mogen gebruiken van opsporingsbevoegdheden (artikel 13), reisbeperkingen (artikel 14), gegevensverwerking (artikel 19), en interne gegevensverstrekking (artikel 48) te gelden.

Artikelen 121 tot en met 123

Artikel 121 regelt de verslaglegging door de CTIVD. Deze regeling is ten opzichte van de bestaande regeling ongewijzigd gebleven. Dit geldt ook voor het bepaalde in artikel 122 inzake de openbaarheid van de gegevens die bij de CTIVD berusten alsmede de toepasselijkheid van artikel 58 op de bij de CTIVD berustende archiefbescheiden. Voorts zijn de in artikel 20 en 21 geformuleerde zorgplichten van overeenkomstige toepassing op de CTIVD.

Artikel 132

In artikel 132, eerste lid, wordt de overtreding van de medewerkingsverplichtingen, zoals opgenomen in de artikelen 29, zesde lid (uitleveren van brieven en andere geadresseerde zendingen), 30, achtste lid (meewerken aan het ongedaan maken van versleuteling), 32, zevende lid (medewerking aan gerichte interceptie door andere aanbieders van communicatiediensten dan de aanbieders van openbare telecommunicatienetwerken en –diensten), artikel 36, vierde lid (verstrekken informatie in verband met toepassing kunnen geven aan artikel 33, eerste lid), 37, vijfde en zesde lid (medewerking aan uitvoering last ex artikel 33, eerste lid, door andere aanbieders van communicatiediensten dan de aanbieders van openbare telecommunicatienetwerken en –diensten onderscheidenlijk de plicht om getroffen voorzieningen van technische aard in stand te houden), artikel 38, vierde lid (medewerking aanbieder van een communicatiedienst aan last om opgeslagen telecommunicatie te verstrekken), 39, vierde lid (medewerking aan last tot verstrekken verkeersgegevens door andere aanbieders van communicatiediensten dan de aanbieders van openbare telecommunicatienetwerken en –diensten), 40, vierde lid (medewerking aan last tot verstrekken abonneegegevens door andere aanbieders van communicatiediensten dan de aanbieders van openbare telecommunicatienetwerken en –diensten), 41, vierde lid (meewerken aan het ongedaan maken van versleuteling), strafbaar gesteld.

In het tweede lid wordt bepaald dat de in het eerste lid strafbaar gestelde feiten misdrijven zijn, voor zover zij opzettelijk zijn begaan. In andere gevallen is sprake van overtredingen. De aard van de delicten – voorkoming of bemoeilijking van het onderzoek door de inlichtingen- en veiligheidsdiensten in het kader van de nationale veiligheid – rechtvaardigt de kwalificatie als misdrijf, indien zij opzettelijk worden gepleegd.

Artikel 134

In dit artikel wordt de toepasselijkheid van de Algemene wet bestuursrecht dan wel het van toepassing zijnde bestuursrecht in de openbare lichamen Bonaire, Sint Eustatius en Saba buiten toepassing verklaard waar het gaat om de voorbereiding, totstandkoming en tenuitvoerlegging van – kort gezegd – de operationele besluiten, zoals bijvoorbeeld inzake de toepassing van bijzondere bevoegdheden, die door de diensten in het kader van de uitvoering van de aan hen opgedragen taken worden genomen.

Artikelen 135 tot en met 144

In deze artikelen worden de daarin opgenomen verwijzingen naar de Wiv 2002 in aangepast aan de tekst van het wetsvoorstel.

Artikel 145

In dit artikel 145 wordt – conform het bepaalde in artikel 99 Wiv 2002 - de in artikel 46 neergelegde plicht tot het uitbrengen van een verslag omtrent de uitoefening van enkele bijzondere bevoegdheden buiten toepassing verklaard voor door de diensten uitgeoefende bevoegdheden voor de datum van inwerkingtreding van de Wiv 2002.

Artikel 146

In artikel 76 van het wetsvoorstel wordt het aangaan van samenwerkingsrelaties met de daarvoor in aanmerking komende diensten van andere landen geregeld. Voorafgaand daaraan dient echter eerst een weging als bedoeld in artikel 67, tweede lid, dienen plaats te vinden, waarbij in ieder geval de in het derde lid opgenomen criteria dienen te worden toegepast. Ingevolge het vierde lid dient de voor de dienst verantwoordelijke minister toestemming te geven voor het aangaan van een samenwerkingsrelatie. Een weging dient opnieuw plaats te vinden indien omstandigheden daartoe aanleiding geven (vijfde lid). In de artikelen 77, zesde lid, en 78, vierde lid, wordt de toestemming voor het verlenen van onderscheidenlijk vragen van ondersteuning aan een dienst van een ander land waaraan risico’s zijn verbonden, voorbehouden aan de voor de desbetreffende dienst verantwoordelijke minister. Op het moment van inwerkingtreding van onderhavig wetsvoorstel zal met betrekking tot diverse bestaande samenwerkingsrelaties van de diensten de ingevolge artikel 76 voorgeschreven weging nog niet hebben

plaatsgevonden. Om te voorkomen dat deze samenwerkingsrelaties in afwachting van een weging zouden moeten worden beëindigd of tijdelijk stopgezet, hetgeen niet in het belang is van de nationale veiligheid, voorziet artikel 146 erin dat genoemde artikelen voor een periode van twee jaar buiten toepassing blijven voor bestaande samenwerkingsrelaties. In deze periode zal derhalve de hier bedoelde weging dienen plaats te vinden.

Artikel 147

De commissie Dessens heeft in haar rapport aanbevolen om in de wet een bepaling op te nemen die enerzijds ziet op een periodieke evaluatie van de wet, en anderzijds op een periodiek onderzoek naar de effectiviteit van het functioneren van de AIVD en de MIVD.[201] In de reactie op het rapport van de commissie Dessens heeft het kabinet aangegeven het passend te achten in de wet een bepaling omtrent een periodieke evaluatie op te nemen. Tevens is daarbij aangegeven dat er nader zal worden bezien hoe en met welke periodiciteit onderzoek wordt uitgevoerd naar de effectiviteit van de diensten. Artikel 147 voorziet in de hier bedoelde evaluatiebepaling, die in twee delen uiteenvalt. Het eerste lid behelst een wetsevaluatie en verplicht de minister-president in overeenstemming met de betrokken ministers binnen vijf jaar na inwerkingtreding van deze wet, en vervolgens telkens na 5 jaar, aan de Staten-Generaal een verslag te zenden over de doeltreffendheid en de effecten van deze wet in de praktijk. Het tweede lid ziet op een evaluatie naar het functioneren van de diensten. Ingevolge het tweede lid zendt de betrokken minister een verslag hieromtrent binnen vijf jaar na inwerkingtreding van deze wet, en vervolgens telkens na vijf jaar, aan de Staten-Generaal. Hiermee wordt voorzien in een systeem waarmee is geborgd dat de bepalingen van deze wet alsmede het functioneren van de diensten periodiek tegen het licht worden gehouden.

Artikel 149

Artikel 149 regelt de nieuwe wettelijke grondslag voor de diverse daarin opgenomen besluiten. De diverse besluiten zullen overigens vooruitlopend op de inwerkingtreding van onderhavig wetsvoorstel worden onderzocht op eventueel benodigde aanpassingen. Er zal naar gestreefd worden de aangepaste besluiten gelijktijdig met de nieuwe wet in werking te laten treden.

[201] Rapport van de commissie Dessens, par. 8.4, blz. 171.

Bijlage 1

Transponeringstabel

Artikel Wiv herzien (doorlopend genummerd)	Artikel huidige Wiv 2002	Wel/niet gewijzigd ten opzichte van huidige Wiv 2002	Omschrijving
1	1	Neen	Definitiebepaling
2	2	Neen	Gebondenheid aan de wet en ondergeschikt aan de betrokken minister
3	3	Ja	Overleg betrokken ministers
4	4	Ja	Coördinator IVD
5			Instelling en taak CVIN
6			Vaststelling geïntegreerde aanwijzing
7	5	Ja	Informatieplicht jegens coördinator
8	6	Ja	Instelling en taak AIVD
9	6a	Neen	Informatie tbv dreigings- en risicoanalyses BB
10	7	Ja	Instelling en taak MIVD
11	7a	Neen	Informatie tbv dreigings- en risicoanalyses BB
12	8	Neen	Jaarverslag diensten
13	9	Ja	Geen bevoegdheid opsporing strafbare feiten
14	10	Ja	Verblijfs- en reisverbod risicolanden
15			Zorgplicht hoofden van dienst voor beveiliging medewerkers
16	11	Neen	Bevoegdheid nadere regelstelling organisatie, werkwijze en beheer diensten
17	12	Neen	Algemene bevoegdheid gegevensverwerking
18	13	Neen	Verwerking persoonsgegevens
19	14	Ja	Van toepassingverklaring 17 en 18 op "RID-en" (artikel 79 en 80), scheiding gegevensverwerking en verantwoordelijkheid archieven
20	15	Neen	Zorgplicht diensthoofden geheimhouding gegevens, bronnen en veiligheid bronnen
21	16	Neen	Zorgplicht diensthoofden voor voorzieningen mbt zorgvuldige gegevensverwerking
22	17	Ja	Algemene bevoegdheid gegevensverzameling
23	18	Ja	Reikwijdte toepassing bijzondere bevoegdheden
24	19	Ja	Toestemmingsregeling bijzondere bevoegdheden
25	20	Neen	Volgen en observeren
26	21	Ja	Inzet agenten
27	22	Ja	Onderzoek van besloten plaatsen, van gesloten voorwerpen, aan voorwerpen en DNA-onderzoek
28			DNA-onderzoek
29	23	Neen	Openen van brieven en andere geadresseerde zendingen
30	24	Ja	Verkennen van en binnendringen in geautomatiseerde werken
31			Definitiebepaling ihkv onderzoek van communicatie
32	25	Ja	Met technisch hulpmiddel gericht aftappen e.d.
33	(deels) 27	Ja	Met technisch hulpmiddel in bulk aftappen e.d. van telecommunicatie of gegevensoverdracht d.m.v. geautomatiseerd werk
34	(deels) 26	Ja	Onderzoek aan ingevolge artikel 33 geïntercepteerde communicatie
35	(deels 27)	Ja	Selectie en metadata-analyse m.b.t. ingevolge artikel 33 geïntercepteerde communicatie

36			Bevoegdheid informatie-inwinning bij resp. informatieplicht van aanbieders van communicatiediensten i.v.m. toepassing artikel 33; kostenregeling
37			Bevoegdheid inroepen van en plicht tot medewerking aanbieders van communicatiediensten i.v.m. toepassing artikel 33; kostenregeling
38			Opvragen opgeslagen gegevens bij aanbieder van communicatiediensten m.b.t. een gebruiker
39	28	Ja	Opvragen verkeersgegevens
40	29	Ja	Opvragen abonneegegevens
41			Medewerkingsplicht ontsleuteling communicatie
42	30	Ja	Toegang tot plaatsen
43	31	Neen	Proportionaliteits- en subsidiariteitstoets
44	32	Neen	Staken bijzondere bevoegdheden bij bereiken doel c.q. inzet minder ingrijpende bevoegdheid
45	33	Neen	Verslag inzet bijzondere bevoegdheid
46	34	Ja	Notificatieplicht
47			Geautomatiseerde data-analyse
48	35	Ja	Regeling interne verstrekking (need to know)
49	36	Ja	Bevoegdheid verstrekking gegevens ihkv goede taakuitvoering
50			Gegevensverstrekking bij verzoek om naslag
51	37	Neen	Voorwaarden aan verder gebruik verstrekte gegevens (w.o. derde partij-regel)
52	38	Ja	Verstrekking gegevens aan met opsporing en vervolging van strafbare feiten belaste instanties
53	39	Neen	Verstrekking ingeval van dringende en gewichtige redenen anders dan i.h.k.v. een goede taakuitvoering
54	40	Neen	Schriftelijke mededeling persoonsgegevens aan instanties die daarop kunnen acteren jegens betrokkene
55	41	Neen	Verstrekking van gegevens waarvan de juistheid redelijkerwijs niet kan worden vastgesteld of ouder zijn dan 10 jaar
56	42	Neen	Aantekening houden van verstrekking persoonsgegevens
57	43	Neen	Verwijdering, vernietiging en verbetering gegevens
58	44	Neen	Afwijking Archiefwet 1995 inzake overbrenging archiefbescheiden
59			Van overeenkomstige toepassing verklaring artikelen 23, 24 en 45 bij inzet overige bijzondere bevoegdheden (geen gegevensverwerking)
60	(deels) 21	Ja	Oprichten en inzet rechtspersonen
61	(deels) 21	Ja	Bevorderen of treffen van maatregelen
62	45	Neen	Bepaling inzake gesloten inzagestelsel
63	46	Neen	Definitiebepaling
64	47	Neen	Aanvraag, behandelingstermijn en inzage eigen persoonsgegevens
65	48	Neen	Afleggen schriftelijke verklaring nav inzage eigen persoonsgegevens
66	49	Neen	Inzage door (oud) medewerkers van de dienst in hem betreffende gegevens in de personeels- en salarisadministratie
67	50	Neen	Aanvraag inzage persoonsgegevens van overleden familieleden (eerste graads)
68	51	Neen	Aanvraag, behandelingstermijn en inzage andere gegevens dan persoonsgegevens (bestuurlijke aangelegenheid)
69	52	Neen	Regeling inzake wijze van kennisneming gegevens
70	53	Neen	Weigeringsgrond eigen persoonsgegevens ivm actueel kennisniveau
71	54	Neen	Weigeringsgrond persoonsgegevens overleden familieleden ivm actueel kennisniveau
72	55	Neen	Absolute en relatieve weigeringsgronden; informatieplicht

			jegens CTIVD bij weigering inzage
73	56	Neen	Beperkingsgronden
74	58	Ja	Samenwerking AIVD en MIVD
75			Informatieplicht over en weer AIVD en MIVD inzake operationele activiteiten (deconflictie)
76	59, eerste lid	Ja	Samenwerking met buitenlandse diensten; afwegingskader; toestemmingsregeling
77	59, tweede tot en met zesde lid	Ja	Verstrekking van gegevens en verlenen van technische en andere vormen van ondersteuning aan buitenlandse diensten
78			Bevoegdheid AIVD en MIVD tot het doen van een verzoek om technische en andere vormen van ondersteuning aan een buitenlandse dienst; toestemmingsregeling; begrenzing bevoegdheid
79	60	Ja	Inzet medewerkers andere instanties onder verantwoordelijkheid min BZK en op aanwijzing hoofd AIVD
80			Inzet medewerkers Kmar onder verantwoordelijkheid min Def en op aanwijzing hoofd MIVD
81	61	Ja	Informatieverplichting openbaar ministerie; overlegregeling diensten – openbaar ministerie
82	62	Ja	Informatieverplichting ambtenaren politie, rijksbelastingdienst en Kmar
83	63	Ja	Technische en andere vormen van ondersteuning (over en weer) diensten – politie/Kmar
84			Grondslag voor nadere regelstelling inzake samenwerkingsverbanden diensten en andere instanties
85[202]	64	Ja	Instelling en taak CTIVD, afdeling toezicht en afdeling klachtbehandeling
86	65, eerste en tweede lid	Ja	Samenstelling en benoeming leden CTIVD en afdelingen
87	65, tweede tot en met achtste lid	Ja	Benoemingsprocedure en vereisten leden
88	66	Ja	Ontslagregeling leden
89	67	Ja	Regeling non actiefstelling
90	68	Ja	Grondslag regeling rechtspositie leden
91	69	Ja	Regeling inzake ondersteuning door secretariaat
92	70	Ja	Overeenkomstige toepassing verblijf- en reisverboden ex artikel 14; ontheffingsbevoegdheid bij minister-president
93	71	Neen	Reglement van orde afdelingen CTIVD
94	72	Ja	Vergaderingen CTIVD en haar afdelingen zijn niet openbaar
95	73	Ja	Informatie- en medewerkingsplicht betrokkenen bij uitvoering Wiv en Wvo
96	74	Ja	Bevoegdheid afdelingen CTIVD oproepen getuigen en deskundigen
97	75	Ja	Afleggen een of belofte getuigen; verplichting onpartijdige taakuitvoering deskundige
98	76	Ja	Bevoegdheid afdelingen CTIVD om bepaalde werkzaamheden aan deskundigen op te dragen

[202] Door de instelling van een tweetal afdelingen bij de CTIVD, waaraan de te onderscheiden onderzoeksbevoegdheden toekomen, zijn de verschillende bepalingen daarop aangepast en als een inhoudelijke wijziging aangemerkt.

99	77	Ja	Binnentredingsbevoegdheid afdelingen CTIVD (m.u.v. woningen)
100	78	Ja	Onderzoeksbevoegdheid wijze uitvoering is gegeven aan Wiv of Wvo i.h.k.v. rechtmatigheidstoezicht; bevoegdheid EK en TK om een onderzoek te vragen; informatieplicht afdeling toezicht CTIVD inzake voorgenomen onderzoek
101	79	Ja	Procedure toezichtsrapport
102			Heroverwegingsregeling m.b.t. verleende toestemming uitoefening desbetreffende bijzondere bevoegdheden; plicht heroverweging minister en informeren van TK bij afwijking van oordeel afdeling toezicht CTIVD
103	83	Ja	Indiening klacht bij afdeling klachtbehandeling; kenbaarheidsvereiste; titel 9.2 Awb n.v.t.; Nationale ombudsman onbevoegd
104			Inhoud klaagschrift
105			Verschoningsregeling medewerken aan behandeling klaagschrift
106			Hoor en wederhoor (klager/bestuursorgaan)
107			Behandeling van de klacht (samenstelling); toepasselijkheid hoofdstuk 2 Awb
108			Doorverwijzingsregeling (indien mogelijkheid van bezwaar, beroep of beklag openstaat)
109			Onbevoegdheid instellen of voortzetten behandeling klacht
110			Niet verplicht instellen of voortzetten klachtbehandeling
111			Niet verplicht instellen of voortzetten klachtbehandeling na bepaald tijdsverloop (een jaar)
112			Mededeling aan klager of bestuursorgaan indien geen onderzoek ingesteld of voortgezet
113			Beoordeling klacht (rechtmatig/behoorlijk); verbinden gevolgen aan oordeel; informeren klager en minister; verplichting minister opvolging oordeel
114			Definitiebepaling bij regeling behandeling van meldingen inzake vermoedens van misstanden
115			Bevoegdheid melden vermoeden van misstand bij afdeling klachtbehandeling; inhoud melding
116			In behandeling nemen melding; informeren minister; bescherming identiteit melder
117			Niet verplicht instellen of voortzetten onderzoek
118			Mededeling aan melder en minister ingeval niet instellen of voorzetten onderzoek naar melding misstand
119			Hoor en wederhoor bij onderzoek melding
120			Onderzoek melding; opstellen rapport; voorleggen concept aan minister voor reactie; vaststelling rapport; verdere procedure en gevolgen oordeel of aanbeveling
121	80	Neen	Jaarverslag CTIVD
122	81	Ja	Gegevens die in het kader van de taakuitvoering aan de CTIVD en haar afdelingen zijn verstrekt zijn niet openbaar
123	82	Neen	Van overeenkomstige toepassing verklaring artikel 20 en 21 op CTIVD
124	85	Neen	Geheimhoudingsplicht
125	86	Neen	Uitzondering geheimhoudingsplicht; verschoningsplicht indien opgeroepen als getuige of deskundige, tenzij er een ontheffing is verleend
126	87	Ja	Geheimhouding inlichtingen en stukken in bestuursrechtelijke procedures
127			Geheimhouding inlichtingen en stukken in civielrechtelijke procedures
128	88	Neen	Beslissing geheimhouding stukken ingeval van inschakeling adviescommissie ex 7:13 Awb voorbehouden aan minister
129	88a	Neen	Wiv van toepassing op de BES

130	88b	Neen	Voor toepassing Wiv is Algemene wet op het binnentreden van toepassing op de BES
131	88c	Ja	Medewerkingsverplichting telecomaanbieders BES bij uitvoering bevoegdheden inzake onderzoek van telecommunicatie
132	89	Ja	Strafbaarstelling niet voldoen aan informatie- en medewerkingsverplichtingen
133	90	Ja	Toepasselijkheid diverse bepalingen op gegevensverwerking door of ten behoeve inlichtingen- en veiligheidsdiensten die zijn opgeheven
134	91	Ja	Buiten toepassing verklaring van de Awb en bestuursrecht BES op operationele besluiten IVD
135			Aanpassing Telecommunicatiewet
136			Aanpassing Aanpassingswet invoering bachelor-masterstructuur
137			Aanpassing Algemene wet bestuursrecht
138			Aanpassing Wet Incompatibiliteiten Staten-Generaal en Europees Parlement
139			Aanpassing Wet politiegegevens
140			Aanpassing Wetboek van Strafrecht
141			Aanpassing Ambtenarenwet
142			Aanpassing Vreemdelingenwet 2000
143			Aanpassing Wet bescherming persoonsgegevens
144			Aanpassing Wet bevordering integriteitsbeoordelingen door het openbaar bestuur
145	99	Ja	Uitzonderen notificatieplicht voor bijzondere bevoegdheden ingezet voor inwerkingtreding Wiv 2002
146			Tijdelijk buiten toepassingverklaring regeling inzake weging en toestemming samenwerking met buitenlandse diensten voor bestaande samenwerkingsrelaties
147			Evaluatiebepaling
148			Intrekking Wiv 2002
149			Nieuwe grondslag uitvoeringsregelingen
150			Inwerkingtredingartikel en vaststellen nieuwe nummering
151			Citeertitel

Bijlage 2

Opbouw wetsvoorstel

Hoofdstuk 1 Algemene bepalingen

Hoofdstuk 2 De diensten en de coördinatie tussen de diensten

Paragraaf 2.1 De coördinatie van de taakuitvoering door de diensten

Paragraaf 2.2 De Algemene Inlichtingen- en Veiligheidsdienst

Paragraaf 2.3 De Militaire Inlichtingen- en Veiligheidsdienst

Paragraaf 2.4 Verslaglegging omtrent de taakuitvoering door de diensten

Paragraaf 2.5 Bijzondere bepalingen betreffende de functionarissen die ten behoeve van de diensten werkzaam zijn

Paragraaf 2.6 Nadere regels met betrekking tot organisatie, werkwijze en beheer van de diensten

Hoofdstuk 3 De verwerking van gegevens door de diensten

Paragraaf 3.1 Algemene bepalingen

Paragraaf 3.2 De verzameling van gegevens

Paragraaf 3.2.1 Algemene bevoegdheid van de diensten

Paragraaf 3.2.2 Bijzondere bevoegdheden van de diensten

Paragraaf 3.2.2.1 Algemene bepalingen

Paragraaf 3.2.2.2 Observeren en volgen

Paragraaf 3.2.2.3 Agenten

Paragraaf 3.2.2.4 Onderzoek van besloten plaatsen, van gesloten voorwerpen, aan voorwerpen en DNA-onderzoek

Paragraaf 3.2.2.5 Openen van brieven en andere geadresseerde zendingen

Paragraaf 3.2.2.6 Verkennen van en binnendringen in geautomatiseerde werken

Paragraaf 3.2.2.7 Onderzoek van communicatie

Paragraaf 3.2.2.7.1 Algemeen

Paragraaf 3.2.2.7.2 Onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers

Paragraaf 3.2.2.7.3 Onderzoek van communicatie in andere gevallen

Paragraaf 3.2.2.7.4 Informatie- en medewerkingsplicht aanbieders van communicatiediensten bij de verwerving van telecommunicatie op grond van artikel 33

Paragraaf 3.2.2.7.5 Informatieverzoeken en medewerkingsplicht met betrekking tot telecommunicatiegegevens

Paragraaf 3.2.2.7.6 Medewerkingsplicht bij ontsleuteling communicatie

Paragraaf 3.2.2.8 Toegang tot plaatsen

Paragraaf 3.2.2.9 Afwegingskader en verslaglegging

Paragraaf 3.2.3 Het uitbrengen van verslag omtrent de uitoefening van enkele bijzondere bevoegdheden

Paragraaf 3.3 Bijzondere bepalingen inzake geautomatiseerde data-analyse

Paragraaf 3.4 De verstrekking van gegevens

Paragraaf 3.4.1 De interne verstrekking van gegevens

Paragraaf 3.4.2 De externe verstrekking van gegevens

Paragraaf 3.4.2.1 Algemene bepalingen

Paragraaf 3.4.2.2 Bijzondere bepalingen betreffende de externe verstrekking van persoonsgegevens

Paragraaf 3.5 De verwijdering, vernietiging en overbrenging van gegevens

Hoofdstuk 4 Overige bijzondere bevoegdheden van de diensten

Paragraaf 4.1 Algemeen

Paragraaf 4.2 Oprichten en inzet van rechtspersonen

Paragraaf 4.3 Bevorderen of treffen van maatregelen

Hoofdstuk 5 Kennisneming van door of ten behoeve van de diensten verwerkte gegevens

Paragraaf 5.1 Algemene bepalingen

Paragraaf 5.2 Recht op kennisneming van persoonsgegevens

Paragraaf 5.3 Recht op kennisneming van andere gegevens dan persoonsgegevens

Paragraaf 5.4 Wijze van kennisneming van gegevens

Paragraaf 5.5 Weigeringsgronden en beperkingen

Hoofdstuk 6 Samenwerking tussen inlichtingen- en veiligheidsdiensten en met andere instanties

Paragraaf 6.1 Samenwerking tussen de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst

Paragraaf 6.2 Samenwerking met inlichtingen- en veiligheidsdiensten van andere landen

Paragraaf 6.3 Samenwerking met andere instanties

Paragraaf 6.4 Nadere regels inzake samenwerkingsverbanden

Hoofdstuk 7 Toezicht, klachtbehandeling en de behandeling van meldingen inzake vermoedens van misstanden

Paragraaf 7.1 Instelling, samenstelling en andere bijzondere bepalingen betreffende de commissie van toezicht

Paragraaf 7.2 De taakuitvoering door de commissie van toezicht

Paragraaf 7.2.1 Algemene bevoegdheden bij toezicht, klachtbehandeling en de behandeling van meldingen inzake vermoedens van misstanden

Paragraaf 7.2.2 De uitoefening van het toezicht door de afdeling toezicht

Paragraaf 7.2.3 De behandeling van klachten door de afdeling klachtbehandeling

Paragraaf 7.2.4 De behandeling van meldingen inzake vermoedens van misstanden

Paragraaf 7.3 Verslaglegging door de commissie van toezicht

Paragraaf 7.4 Overige bepalingen met betrekking tot de commissie van toezicht

Hoofdstuk 8 Geheimhouding

Hoofdstuk 9 Bonaire, Sint Eustatius en Saba

Hoofdstuk 10 Straf-, overgangs- en slotbepalingen

Bijlage 3 Overzicht bijzondere bevoegdheden en waarborgen

Bijzondere bevoegdheid[203][204]	**Instantie die toestemming verleent**	**Duur**	**Toets**	**Bewaartermijn c.q. vernietigingstermijn gegevens**	**Functiescheiding/ taakscheiding/ compartimentering**
Observeren en volgen (artikel 25)	Minister of hoofd dienst; ondermandaat mogelijk. Minister indien inzet technische hulpmiddelen in woningen betreft.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Niet van toepassing
Agenten (artikel 26)	Minister of hoofd van dienst; ondermandaat mogelijk	Max. een jaar; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Niet van toepassing.
Doorzoeken besloten plaatsen; doorzoeken gesloten voorwerpen; verrichten van onderzoek aan een voorwerp gericht op vaststellen identiteit (artikel 27)	Minister of hoofd dienst; ondermandaat mogelijk. Minister indien het doorzoeken van woningen betreft.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Niet van toepassing.
DNA-onderzoek gericht op vaststellen (inclusief verificatie) identiteit (artikel 28)	Minister. Ook waar het gaat om verdere verwerking van resultaten DNA-onderzoek betreft.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk. Naar zijn aard echter geldig voor een specifiek onderzoek.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Celmateriaal dat gebruikt is voor DNA-onderzoek dient binnen drie maanden daarna te worden vernietigd. DNA-profielen mogen max. 5 jaar worden bewaard; verlenging mogelijk met toestemming minister.	Toegang tot de gegevens wordt bij algemene maatregel van bestuur ingekaderd.
Openen van brieven en andere geadresseerde zendingen (artikel 29)	Rechtbank Den Haag	Voor een brief of andere geadresseerde zending in bezit van de dienst: per brief of geadresseerde zending. In overigen gevallen: max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Niet van toepassing.
Verkennen en binnendringen van geautomatiseerde werken; medewerkingsplicht derden bij ontsleuteling (artikel 30)	Minister; ook waar het gaat om de medewerkingsplicht bij ontsleuteling.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Uit geautomatiseerde werken overgenomen gegevens dienen binnen twaalf maanden op relevantie te worden onderzocht en daarna te worden vernietigd.	Niet van toepassing.
Onderzoek van communicatie m.b.t. specifieke personen, organisaties en nummers (artikel 32)	Minister. Geen toestemming vereist bij militair verkeer met oorsprong of bestemming in andere landen.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Verkregen gegevens dienen binnen twaalf maanden op relevantie te worden onderzocht en daarna te worden vernietigd. Ingeval van toepassing bevoegdheid m.b.t. militair verkeer dient niet-militair verkeer terstond te worden vernietigd.	Niet van toepassing.
Onderzoek van communicatie in andere gevallen (artikel 33)	Minister.	Max. 12 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Verkregen gegevens mogen voor een periode van ten hoogste van drie jaren	Ja. Minister wijst ambtenaren aan die kennis mogen nemen van de gegevens ten

[203] Voor zover uitoefening plaatsvindt jegens een journalist, waarbij de uitoefening is gericht op het achterhalen van de bron van de journalist, is toestemming van de rechtbank Den Haag vereist.

[204] Voor zover de uitoefening plaatsvindt ter ondersteuning van een goede taakuitvoering van de diensten (artikel 23, tweede lid), dan is toestemming vereist van de minister; duur toestemming is gesteld op max. 1 maand met mogelijkheid van verlenging; CTIVD wordt van verleende toestemming op de hoogte gesteld. (artikel24, vijfde lid).

				worden bewaard t.b.v. een verwerking als bedoeld in artikel 34 en 35; niet-relevante of niet op relevantie onderzochte gegevens worden daarna vernietigd.	behoeve van de in dit kader benodigde werkzaamheden. Mandaat aan hoofd van de dienst mogelijk.
Onderzoek aan gegevens verworden o.g.v. artikel 33: search gericht op interceptie en search gericht op selectie (artikel 34)	Minister.	Max. 12 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Zie regeling bij artikel 33.	Ja. Minister wijst ambtenaren aan die kennis mogen nemen van de gegevens ten behoeve van de in dit kader benodigde werkzaamheden. Mandaat aan hoofd van de dienst mogelijk.
Selectie van gegevens; metadata-analyse (artikel 35)	Minister voor selectie van gegevens; minister voor metadata-analyse gericht op identificeren van personen of organisaties.	Max. 3 maanden met verlengingsmogelijkheid (selectie); Max. 12 maanden met verlengingsmogelijkheid (metadata-analyse).	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Zie regeling bij artikel 33.	Ja. Minister wijst ambtenaren aan die kennis mogen nemen van de gegevens ten behoeve van de in dit kader benodigde werkzaamheden. Mandaat aan hoofd van de dienst mogelijk.
Informatieplicht aanbieder van communicatiediensten i.v.m. toepassing artikel 33 (artikel 36)[205]	Geen toestemming vereist. Verzoek aan aanbieder geschiedt door hoofd van de dienst.	Niet van toepassing.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Niet van toepassing.
Medewerkingsplicht aanbieder van communicatiediensten bij uitvoering verleende toestemming ex artikel 33, tweede lid (artikel 37)[206]	Minister.	Max. 12 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Niet van toepassing.
Opvragen opgeslagen telecommunicatie van een gebruiker bij een aanbieder van een communicatiedienst (artikel 38)	Minister.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Verkregen gegevens dienen binnen twaalf maanden op relevantie te worden onderzocht en daarna te worden vernietigd.	Niet van toepassing.
Opvragen verkeersgegevens bij aanbieder van communicatiediensten (artikel 39)	Minister of namens deze het hoofd van de dienst.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Niet van toepassing.
Opvragen abonneegegevens bij aanbieder van communicatiediensten (artikel 40)	Geen toestemming vereist.	Niet van toepassing.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Niet van toepassing.
Medewerkingsplicht bij ontsleuteling gegevens verkregen op grond van artikel 32 en 33 (artikel 41)[207]	Minister.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Niet van toepassing.
Toegang tot plaatsen (artikel 42)[208]	Geen toestemming vereist. Wel machtiging tot binnentreden van een woning zonder toestemming bewoner vereist, af te geven door minister of namens deze het hoofd van de dienst (Algemene wet op het binnentreden).	Machtiging tot binnentreden is drie dagen geldig (Algemene wet op het binnentreden).	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Uitoefening van de bevoegdheid ex artikel 42, eerste lid, is alleen toegestaan door personen die daartoe door hoofd van de dienst zijn aangewezen.

[205] Ondersteunende bevoegdheid.

[206] Ondersteunende bevoegdheid.

[207] Ondersteunende bevoegdheid.

[208] Ondersteunende bevoegdheid.